

Privacy Impact Assessment (PIA)



Disaster Credit Management System (DCMS)

Office of Disaster Assistance

James E. Rivera

**U.S. Small Business Administration
409 Third Street, SW
Washington, DC 20416**

Name of Project: Disaster Credit Management System (DCMS)

Program Office: Office of Disaster Assistance

Project's Unique ID: 028-00-01-05-01-5001-00-104-009

A. CONTACT INFORMATION

1) Who is the person completing this document?

Michael Yeager
Director, DCMS Operations Center
13221 Woodland Park Road
Herndon, VA 22171
(703) 487-6644
Michael.Yeager@sba.gov

2) Who is the system owner?

James E. Rivera
Associate Administrator for Disaster Assistance
Small Business Administration (SBA)
409 3rd Street, S.W.
Washington, DC 20416
(202) 205-6734
James.Rivera@sba.gov

3) Who is the Sr. Advisor who reviewed this document?

Ethel Matthews
Sr. Privacy Advisor
Office of Chief Information Officer
409 3rd Street, S.W.
Washington, DC 20416
(202) 205-7173

4) Who is the Reviewing Official?

Paul T. Christy
Chief Information Officer
Small Business Administration

409 3rd Street, S.W.
Washington, DC 20416
(202) 205-6756
Paul.Christy@sba.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) Does this system contain any information about individuals?

Yes.

DCMS contains information on personal residence, employment, assets, income, expenses, taxes, credit history, property, and disaster damage is collected and used in the system in making disaster loan application decisions for the general public that file applications for disaster loans.

Information on employees is also tracked, personal information, emergency contacts, personnel data, accountable property and computer access.

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 system is used to process loan applications and determinations for the disaster loan program. The information is based on the specific need to evaluate program eligibility disaster damage, credit worthiness, repayment, statutory interest rate, character and eligibility as defined in the Small Business Act and 13 CFR.

The system is also used to manage information about ODA staff and contractors – including names, social security numbers, accountable property, home offices and assigned system accounts.

3) Is the system in the development process?

No

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

Currently DCMS is in the maintenance mode of its lifecycle and no technology investments are foreseen at this time.

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 Protection Act of 1988)

Paperwork Reduction Act of 1995; 44 USC 3501.

Government Paperwork Elimination Act of 1998.

Federal Records Act of 1950 and National Archives and Records Administration (NARA) implementing regulating at 36 CFR 1220 and 41 CFR 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 management (for example, the Paperwork Reduction Act, the Clinger-Cohen Act; and the Government Performance and Results Act).

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?

For the Electronic Loan Application (ELA), to prevent partially completed loan applications from being accessed by anyone but the applicant, the data is deleted from

the public-facing portion of DCMS as soon as the applicant submits it as completed. Data not yet submitted as complete is deleted after the Application Deadline date. Also, we require an independent service to identify the person applying and two-factor authentication for all these people to sign on to the system.

To prevent data on system backup tapes from being compromised, the tapes are encrypted.

To ensure data extracts containing PII are not exposed for any longer a period than necessary, they are identified, tracked, and deleted once their expiration dates are reached.

To ensure employees do not view PII data not required in the performance of their jobs, DCMS user accounts are assigned specific roles and responsibilities. Users are limited in their access to areas of the system appropriate for those responsibilities.

C. SYSTEM DATA

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

The categories of individuals would be members of the general public who are disaster victims and that apply for disaster loans, and individuals who have worked for the SBA Office of Disaster Assistance, either as employees or as contractors.

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

Information is collected directly from disaster victims that apply for disaster loans, from Federal Emergency Management Agency (FEMA), the Internal Revenue Service (IRS), from commercial vendors of credit-related information, and from the National Flood Insurance Program (NFIP).

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?

Information is collected from several sources: directly from disaster victims that apply for disaster loans, from the Federal Emergency Management Agency (FEMA) by way of electronic referral resulting from the applicant applying for disaster assistance through FEMA, the Internal Revenue Service (IRS), from commercial vendors of credit-related information, and from the National Flood Insurance Program (NFIP).

Employee information is collected from several sources: employment applications and paperwork, electronically from the FBI for fingerprint checks, from Credit Bureau Agencies for credit worthiness.

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

The federal agencies are FEMA, IRS and the Department of Justice.

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

State or local agencies which develop grant programs for future disasters may provide data from time to time, as these programs are developed for specific disasters.

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

Commercial credit bureaus (various), Dun & Bradstreet business reports, commercial vendors of reference data (Zip Codes), commercial vendors of flood plain mapping data, insurance companies, etc.

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

The applicant provides their name, social security or EIN number, address, contact information, employment, asset, income, expense, tax, property and disaster damage data. The data is collected via an OMB approved form, referenced as OMB No. 3245-0017, and via a public-facing web-based interface.

The employee provides their Social Security Number, address, contact information, prior employment records. The data is collected via employment application and acceptance forms.

3) Accuracy, Timeliness, and Reliability

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

Most of the data is collected from the applicants via a web-interface or via a paper application. In either case, the applicant verifies the data before submission to the SBA. DCMS also receives data from other trusted Federal agencies, e.g., FEMA and the IRS, as well as from private credit bureaus, such as Experian and Equifax. Each of these entities takes responsibility for verifying the data for accuracy that they send to the SBA.

b. How is data checked for completeness?

Data is contained in a loan application completed either via a web interface or on paper. An authorized individual, i.e., a Loan Officer in the employ of SBA, reviews the application for completeness. If any data is missing, the Loan Officer contacts the applicant to obtain the missing information before processing the application.

c. Is the data current?

Yes. Credit Bureau and business report data captures the date of entry for all line items or general updates. IRS and FEMA data is updated as needed to ensure current values. Data collected directly from applicants, SBA ODA employees and contractors is updated as provided.

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

Yes. All data elements are listed in a DCMS data dictionary.

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

DCMS collects information on applicants and staff which includes PII. PII could be disclosed to unauthorized third parties.

Mitigation steps include the following:

- Agreements (MOUs) are concluded with Federal agencies and organizations that require DCMS data. Clauses that protect the handling of PII are included in these agreements.
- Electronic data is transferred via secure interfaces, including VPN and secure leased lines.
- DCMS does not provide other systems access to the entire DCMS database, but only to a subset of the data which has been identified as critical to their mission.
- DCMS staff receive annual Computer Security Awareness Training, which includes a comprehensive module on the handling and protection of PII.
- Certain data fields are unavailable based upon user roles and responsibilities.
- Recipients of PII are informed of their responsibilities for protecting the data and for deleting it after a defined period.

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. The information is based on specific need to evaluate disaster damage, credit worthiness, repayment, statutory interest rate, character and eligibility as defined in the Small Business Act and 13 CFR.

- 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.

- 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?**

N/A

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

All loan process data is resident on one system, with User ID and role-based access controls.

- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? If process are not be 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.**

Data is accessed by authorized users with sufficient privileges by name, agency application number, address or SSN/EIN.

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

No reports on individuals are created at this time. Ad-hoc reports can be produced on individuals but only by order of authorized SBA staff and managers and on a ‘need-to-know’ basis. The reports are then created by authorized SBA staff. Only these authorized individuals have access to the reports.

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.

Applications for disaster loans are voluntary. The data collected via the application form is required for the loan determination process.

Most of the data collected on employees and contractors is mandatory for employment consideration. Where specific data elements on the employment application and hiring paperwork are identified to not be required or are listed only ‘if applicable,’ the individual has the option to not provide any information.

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

Before gaining access to DCMS, all users sign a “Rules of Behavior” form which states, in part, that they are prohibited from accessing or attempting to access systems or information for which they are not authorized. The form stipulates that users may not read, store or transfer information for which they are not authorized, and that disciplinary action may result from any unauthorized use of SBA systems and computer resources for non-work-related activities. In signing the form, users state that they have read and understand their responsibilities and will comply with the form’s rules.

User access is based on need-to-know and the role of the position the employees are assuming. Therefore, staff only can access PII that they definitely need in the performance of their work.

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 system operates from a single site with a separate site as a backup. Data is replicated to the backup site for disaster recovery purposes.

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

Data is retained until it is no longer needed for operations or reference. The retention periods are defined in SBA's Privacy Act Systems of Record, SBA 20 and SBA 21. In accordance with SBA Standard Operating Procedure 0041 2, Item Nos. Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18, and 21.

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 disposition of data at the end of retention is by sanitation; which includes degaussing of magnetic media or final destruction of the media by shredding or combustion. In accordance with procedures documented in several of the Office of Management and Budget (OMB) memoranda including OMB Memorandum M-10-22, published June 25, 2010, all government agencies are required to implement procedures to safeguard Agency sensitive information and PII. DCMS complies with this requirement and keeps reports for a maximum of 90 days.

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.

No

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

N/A

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

N/A

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

System of Records notice (SORN) SBA-20

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

No revision is necessary.

F. DATA ACCESS

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

Agency officials and certified contractors will have access to data in the system. Access is limited to Agency officials acting in their official capacity, with a need to know, and certified contractors under confidentiality agreements while actually engaged in system development, modification or maintenance. This may include users, managers, or system administrators.

- 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 individual's role and responsibility. Access is limited by control of User IDs, password controls, and the assignment of a Responsibility profile to all User IDs. 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. User access policies and procedures for DCMS have been published.

- 3) **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 level of system responsibility assigned users by their managers and approved by the DCMS System Security Officer.

- 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)**

Access is limited by control of User IDs, password controls, and the assignment of a Responsibility profile to all User IDs, effectively limiting browsing. Education of Agency and contractor staff regarding the Privacy Act rules and prohibitions on the dissemination or use of non-public information is mandatory and ongoing. System audit trails can be used to document suspicious or irregular logons 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 System of Records SBA 20 defines routine uses of this information and serves as a control by defining acceptable uses. Limiting access to sensitive information to only those with a need to know remains the best and primary control.

- 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?**

Yes, contractors are involved in the design, development, and maintenance of the system. Yes, clauses are in the contracts that protect Privacy Act and other sensitive data.

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

Yes. When authorized by management, processes have been created to exchange specific items of data from, or to, other systems. The agreed upon data is transmitted as discrete packets sent over secure interfaces.

No other system has access to the data in the system. All shared data is “pushed” to other systems.

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

The DCMS 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))?**

No other system has access to the data in the system. Data is periodically shared with other systems from Federal and State agencies to help expedite disaster recovery processes. Generally, requests are received for specific information from other entities. Sufficient information must be provided to verify the specific records

requested within DCMS. Discrete packets of specific data are provided only relative to the verified records. All information requests are cleared through the appropriate Agency Offices.

Data is also shared with the FEMA NEMIS system. Agreed upon data elements are transmitted as discrete packets sent over secure interfaces. This use is in accordance with SBA Privacy Act System 20.

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

FEMA and State Agencies use the data to implement statutory prohibitions on Duplication of Benefits to disaster victims. Where appropriate, Computer Matching Agreements exist to ensure shared data is correctly paired by the recipient to data obtained through other channels.

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

FEMA has authority to obtain the data for established uses and FEMA assumes responsibility (under the Privacy Act) for its use once obtained. The exchange of data between FEMA and SBA and responsibilities for protection of privacy data are defined in a Memorandum of Agreement, a Computer Matching Agreement and an Interagency Security Agreement as accepted by FEMA and SBA security officers and formally agreed to and signed by the Chief Information Officers of FEMA and SBA. Administration of DCMS security policies is the responsibility of the DCMS Security Officer.

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

DCMS collects information on applicants and staff which includes PII. PII could be disclosed to unauthorized third parties.

Mitigation steps include the following:

- Agreements (MOUs) are concluded with Federal agencies and organizations that require DCMS data. Clauses that protect the handling of PII are included in these agreements.
- Electronic data is transferred via secure interfaces, including VPN and secure leased lines.
- DCMS does not provide other systems access to the entire DCMS database, but only to a subset of the data which has been identified as critical to their mission.

- DCMS staff receive annual Computer Security Awareness Training, which includes a comprehensive module on the handling and protection of PII.
- Certain data fields are unavailable based upon user roles and responsibilities.
- Recipients of PII are informed of their responsibilities for protecting the data and for deleting it after a defined period.

Privacy Impact Assessment (PIA) Approval Page

Name of Project: Disaster Credit Management System (DCMS)
Program Office: Office of Disaster Assistance

The Following Officials Have Approved this Document:

1) System Owner

James E. Rivera (Signature) 10/25/11 (Date)

Name: James E. Rivera

Title: Associate Administrator for Disaster Assistance

2) Chief Privacy Officer

Paul T. Christy (Signature) 10/25/11 (Date)

Name: Paul T. Christy

Title: Chief Information Officer / Chief Privacy Officer