

SBA DCMS PIA

SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

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

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Michael Sorrento
Director DCMS Operations Center
SBA Office of Disaster Assistance
703-487-8100, ext 6644
Michael.Sorrento@sba.gov

2) Who is the System Owner?

Herbert L. Mitchell
Associate Administrator for Disaster Assistance
SBA Office of Disaster Assistance
202-205-6734
Herbert.Mitchell@sba.gov

3) Who is the System Manager for this system or application?

Michael Sorrento
Director DCMS Operations Center
SBA Office of Disaster Assistance
703-487-8100, ext 6644
Michael.Sorrento@sba.gov

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

Christopher Rudek
DCMS System Security Officer
SBA Office of Disaster Assistance
703-487-8100 ext 6664
Christopher.Rudek@sba.gov

5) Who is the Bureau/Office Privacy Act 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? (According to OMB, this the agency IO or other agency head designee who is other than the official procuring the system or the official who conducts the PIA).

Christine Liu
Chief Information Officer/Chief Privacy Officer
Office of the Chief Information Officer
202-205-6708
Christine.Liu@sba.gov

B. PIA PROCESS APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

a. Is this information identifiable to the individual!?

Yes

b. Is the information about individual members of the public?'

Yes.

c. Is the information about employees?

Yes.

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

The system is used to process loan 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.

3) What: legal authority authorizes the purchase or development of this PIA Process?

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

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 CSR 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.

C. DATA in the SYSTEM:

- 1) Generally describe the type of information to be used in the system and what categories of individuals are covered in the System?**

Information on 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 include personal information, emergency contacts, personnel data, accountable property and computer access assigned to an individual, personnel history including field duty locations, training and suitability status.

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

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

FEMA NEMIS system, FEMA National Flood Insurance Program (NFIP), and IRS tax transcripts

FBI for employee fingerprint checks

c. What State and local agencies are providing data for use in the process?

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 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 will data collected from sources other than SBA records be verified for accuracy?

Data from Federal Agency records is identified by name, address, and/or SSN and is subject to Privacy Act regulation and documented practices for accuracy. Data from commercial entities is subject to regulation and identified by name, address and SSN. Where commercial credit information results in adverse decisions, applicants are advised of the source of the information and may obtain it through various means at no cost.

b. How will data be checked for completeness?

Applicant data is compared and reconciled with any third party data received. Agency business rules and system edits require critical information be complete before processing. Discrepancies are discussed with applicants.

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)

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 insure current values. Data collected directly from applicants is updated as provided.

d. Are the data elements described in detail and documented? If Yes, What is the name of the document?

Yes, there are several documents that describe data stored in DCMS, data collected from federal agencies, and data collected from commercial sources. Data housed by SBA ODA in DCMS is described in the "Disaster Credit Management System (DCMS) Data Relationship Model" as produced in September 2004 by SRA International, Inc. as a deliverable document for Contract Number *GS07T-00BGD0064/Task Order Number T0003AJL017*, and referenced as DRM-2239021-v2.0. The data interchange with FEMA's NEMIS system is described in the "DCMS 1.0 Implementation FEMA Interface Technical Design" as maintained by SRA International, Inc. as a deliverable for the same contract and is referenced as SDTD-2239002-v2. A similar document describing the internal SBA interface between DCMS and DCS is maintained by SRA International, Inc. as "DCMS 1.0 Implementation DCS Interface Technical

Design" as a deliverable for the same contract. Employee data stored in DCMS is described in DCMS Resource Management Technical Reference Guide, September 2006

D. ATTRIBUTES OF THE DATA

- 1) Is the use of the data both relevant and necessary to the purpose for which the process 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/public that would not be possible without the new data?**

N/A

- 5) How will the new data be verified for relevance 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?**

The DCMS system consolidates data previously housed in multiple legacy systems. All loan process data is resident on one system, with User ID and Responsibility based access controls.

- 7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.**

No processes are being consolidated. Not applicable.

- 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?**

DCMS does not currently generate reports specific to individual loans. Reports can be produced on individual's records for the purpose of workload management and inquiries which comply with FOIA and Privacy Act requirements. Access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

Staffing Reports are generated for individual offices. These reports will be used for the daily operation of the offices and other staff management purposes. These reports are restricted to specific office management and individuals involved with insuring accuracy of the data.

- 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.

The collected employee data which is stored electronically is the same mandatory data required 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.

E. **MAINTENANCE AND ADMINISTRATIVE CONTROLS**

- 1) **If the information in the process is operated in more than one site, how will consistent use of the 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 the system?**

Data retention standards consistent with SOP 00 41 2 are currently being developed. The duration of SBA's interest in approved loans partially dictates the retention standards, i.e. some records will need to be maintained for the life of a loan.

- 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?**

Most reports are updated daily with previous versions deleted at the time of the update. Electronic records and backups are retained for historical purposes and will not be destroyed.

Distributed reports and other data extracts which contain PII or sensitive data are tracked and disposed of in accordance with procedures described in ODA Numbered Memo #08-17. The normal retention period for data extracts is 90 days.

Current processes address the archival of loan processing data with long-term disposition of electronic records in planning. Documentation of the archival process including procedures for disposition of data and report retention standards are partially completed.

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

Future enhancements may utilize technologies not previously employed. However, no current use of technology can be characterized as such to date.

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

N/A

- 6) **Will this system in the processes provided have the capability to identify, locate, and monitor individuals? If yes, explain**

N/A

- 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 does the system operate? Provide number and name**

SMALL BUSINESS ADMINISTRATION Privacy Act System of Records
SBA 20, Disaster Loan Case Files

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

No revision is necessary. While the system is new, the types of data collected and the handling of privacy data remain the same as with the legacy system.

F. ACCESS TO DATA:

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

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 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. A memo detailing DCMS User Access Policies and Procedures was published in August of 2006 as "DCMSOC #06-07, Updated DCMS User Access Policy and Procedures."

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

Users have access only to screens, reports and data corresponding to the assigned system Responsibility the user holds. Managers have control over assigned responsibilities, through authorized system administrators.

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

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 log-ons 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.**

Discreet packets of specific data are sent out to effect interfaces with the Agency DCS system.

No other system has access to the data in the system.

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

N/A

- 8) **Will other agencies share data or have access to the data in this: system?**

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

Discreet packets of specific data are sent out to effect interfaces with the FEMA NEMIS system. This use is in accordance with SBA Privacy Act System 20.

9) **How will the 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.

10) **Who is responsible for assuring proper use of the 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 and 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.

G. Privacy Impact Analysis

1) **Discuss what privacy risks were identified and how they were mitigated for types of information collected.**

Because DCMS now has a public-facing website with a greater risk of disclosing PII to unauthorized individuals, DCMS collects only information that is essential to the disaster loan making process. Deliberate thought was given to the type of data collected during the requirements generation process.

2) **Describe any types of controls that may be in place to ensure that information is used as intent.**

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.

3) **Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?**

MOUs are established with Agencies and organizations that require DCMS data.

Electronic data is transferred via secure interfaces, including VPN and secure leased lines.

DCMS does not give other systems access to the full database but, rather, to a subset of the data identified as required for their mission.

Recipients of PII are informed of their responsibilities for protecting the data and for deleting it after a defined period.

4) **What privacy risks were identified and describe how they were mitigated for security and access controls?)**

For the 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.

APPENDIX A

DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the Small Business Administration to the public and are the responsibility of all SBA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the SBA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of SBA data systems, processes and facilities.

All SBA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the SBA, the SBA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.
Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the SBA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any SBA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.

Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.
---------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the SBA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B
POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The SBA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the SBA recognizes that compliance with legal requirements alone is not enough. The SBA also recognizes its social responsibility which is implicit in the ethical relationship between the SBA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the SBA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the SBA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.


The SBA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. SBA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the SBA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the SBA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the SBA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.

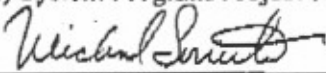
SBA DCMS

The following officials have approved this document:

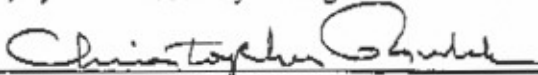
1) System Owner


Name: Herbert L. Mitchell,
Title: Associate Administrator for Disaster Assistance

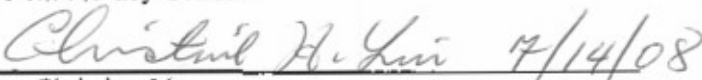
2) System Program/Project Manager


Name: Mike Sorrento
Title: Director, DCMS Operations Center

3) System IT Security Manager

 6-23-08
Name: Christopher Rudek
Title: DCMS Security Officer

4) System Privacy Official

 7/14/08
Name: Christine Liu
Title: Chief Privacy Officer