PRIVACY IMPACT ASSESSMENT

Name of System/Application: CRM-Correspondence Management
Program Office: Office of the Executive Secretariat

A. CONTACT INFORMATION

1) Who is the person completing this document?

Mathilda Hunter
Information Technology Specialist
202-205-7041
Mathilda.Hunter@sba.gov

2) Who is the system owner?

Kim Bradley
Director, Executive Secretariat Office
202-205-2410
Kim.Bradley@sba.gov

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

Mathilda Hunter
Information Technology Specialist
202-205-7041
Mathilda.Hunter@sba.gov

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

Dave McCauley
Chief Information Security Officer
Office of the Chief Information Officer
202-205-7130
David.McCauley@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 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, information that is received will include individuals' names, business addresses, home addresses. this information can be in paper form or email.

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 CRM-Correspondence Management (CRM-CM) system will efficiently manage, organize, search, track, and report on correspondence and action plans. This will enable better responses to customers and stakeholders. The web-based application is a system used to control all correspondence from the public, members of Congress, and Administration officials to and from the Administrator or the Deputy Administrator. The application is also used to control and track all policy/decision documents for the Administrator's or the Deputy Administrator's signature. Correspondence from members of Congress to any SBA official is also controlled and tracked through this system.

3) Is the system in the development process?

1. Yes, (CRM-CM) is in the development process. This system is an additional feature of the CRM project. The CRM project has a draft Privacy Impact Assessment submitted as well as a System Security Plan on file.
2. The system does not require Personally Identifiable Information (PII): there are no fields for SSNs, DOB, etc.; however, some documents that are uploaded in the system contain privacy information.
3. System updates and designs were complete during User Acceptance Testing to include correspondence retention period in accordance with NARA schedule as described in the SBA's SOP 41 (2).

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

The Correspondence Management system is designed to replace the SBA's existing Controlled Correspondence Tracking System. Since it captures the same information, there is no significant impact to privacy in the functioning of the system.

From an infrastructure standpoint, the Correspondence Management system is an integrated module within SBA's CRM system. The CRM system will be hosted on hardware at Engage's secure hosting facility, located in Atlanta, Georgia, with a backup/disaster recovery site located in Dallas, Texas. The following software components and versions will be installed and maintained on the hardware servers located at Engage's secure hosting facility.

The choice for cloud-based hosting at Engage's data center was made to take the burden of maintaining and securing infrastructure off of SBA and ensure more robust and secure infrastructure management from a team dedicated to application hosting.

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.
- 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 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 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 risk identified is limited to the transfer of the records from the SBA LAN to the Engage Data Center. This risk is mitigated, as end-user access to these environments is granted on an individual basis, according to a pre-defined system security process.

C. SYSTEM DATA

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

The CRM-CM will store and manage correspondence from the members of the U.S. House of Representatives and the U.S. Senate, the President, and SBA's Administrator or Deputy Administrator. This correspondence might include attachments that could contain PII from individuals who contacted their Congressional representative(s), or the Administrator concerning various personal or business issues affecting them.

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, then what other source?

Correspondence information is collected from several sources: directly from members of the U.S. House of Representatives and the U.S. Senate, the President, SBA's Administrator or Deputy Administrator, and the general public or SBA's Program Offices.

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

The Federal agencies that may provide data which would be used in this process may include correspondence from the White House, members of Congress, OMB, OPM, and SBA's Administrator.

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

Any Tribal, State, and local agencies could provide data.

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

Third party sources can be the general public and small business proprietors.

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

Information received from the employee or public contained in the system will include: names, home addresses, business addresses, contact information, and various personal or business issues affecting them.

3) Accuracy, Timeliness, and Reliability

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

Data from federal agency records is identified by name and address, 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 other contact information.

b. How is data checked for completeness?

The Executive Secretariat Systems Administrator or Managers will conduct periodic assessments (audits) of the information in the system to determine data accuracy.

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. Data is collected directly from members of the U.S. House of Representatives and the U.S. Senate, the President, SBA's Administrator or Deputy Administrator and the general public, or SBA's Program Offices. The CRM-CM Agency Database Hourly Transaction Logs and Daily incremental backups help system administrators monitor the timeliness of data entries and give them the ability to determine whether data is inactive or out-of-date.

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

Yes. The Engage, Inc. system support maintains the data dictionary for the system elements in the IT Configuration Plan.

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

CRM-CM is primarily a management tool, and access to the information contained in the system is restricted by security roles. Most of the risks identified involved the technological aspects of the design, development, and maintenance of the system. Deliberate thought was given to the type of data collected during the requirements-generation process. All users must acknowledge and accept the prescribed warning regarding misuse of the information contained in this system.

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 system contains set fields that only collect information which is sufficient to identify and track the course of assigned cases.

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 new data will be created—the data already exists in CCTS.

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?**

No data is being consolidated. The old legacy system data will be migrated to CM. All data will reside on one system, with User ID, password, and role 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? If processes are not being consolidated please state, "N/A".**

Processes are being consolidated and the proper controls are being rolled up under CRM system authorizations.

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 based on user ID.

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

Reports can be produced on Program Offices for the purpose of workload assessment. Access is restricted to Executive Secretariat officials. The Daily Congressional Report is generated for active cases, and SBA's Administrator will have access to this.

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.**

N/A

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

The system is a single one: before accessing the SBA's network, all users accept a "Rules of Behavior" contained in the security warning banner which states, in part, that they are prohibited from accessing or attempting to access system 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 accepting this agreement, users state they have read and understand their responsibilities and will comply with the outlined rules.

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 retention standards are consistent with SBA's SOP 41 (2), which requires record management data to be maintained on Administrator's records for a period of three years.

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 Office of the Executive Secretariat archives cases in the system in accordance with the NARA Retention Schedules as describes in the SBA's SOP 41 (2). Reports are maintained indefinitely.

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

There is no additional monitoring software, smart cards, or caller id. This data already resides in an existing system.

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. Names and addresses are a part of the dataset.

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?**

Access is limited by control of User IDs, password controls, and the assignment of a User Role profile to all User IDs, effectively limiting browsing. Executive Secretariat System Administrators and the Database Administrator will use audit logs 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. Training of system users will occur before initial system deployment, with refreshers on-demand.

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

SBA 8 – Correspondence and Inquiries.

10) **If the system is being modified, will the Privacy Act SORN require amendment or revision?**

N/A

F. DATA ACCESS

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

CRM-CM SBA employees designated as Managers or Liaisons in the Program Office, Executive Secretariat staff, and certified contractors under a non-disclosure agreement while actually engaged in system development, modification, or maintenance will have access.

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 User Role profile to all User IDs or Workgroups. Each user role 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 CRM- CM user manual will detail the various roles within the system and explain the access associated with each User Role profile.

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

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

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 User Role profile to all User IDs, effectively limiting browsing. Executive Secretariat System Administrators and the Database Administrator will use audit logs 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. Training of system users will occur before initial system deployment, with refreshers on-demand.

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. Each contractor involved with the system has/is required to complete an SBA 1228, Computer Access-Clearance Security Form certifying they understand and agree to protect Privacy Act and other sensitive data in accordance with the Privacy Act of 1974 and SBA regulations.

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

No, to date, there is no other data system interface.

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

All users of the system will be responsible for privacy and security of data.

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 Federal and State agencies following the proper procedures to redact PII, as required. All information requests are cleared through the appropriate Agency Offices.

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.

Laws, rules, and government-wide regulations that dictate the use of the system data are established.

Electronic data can be accessed and retrieved via secure interfaces, including VPN and secure leased lines.

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

The Following Officials Have Approved this Document:

1) **System Owner**

Kim J. Bradley (Signature) Feb. 19, 2010 (Date)

Name: Kim Bradley

Title: Director, Executive Secretariat

2) **Project Manager**

Mathilda Hunter (Signature) Feb 19, 2010 (Date)

Name: Mathilda Hunter

Title: Information Specialist

3) **IT Security Manager**

for CISO Doug Thompson (Signature) 2/19/10 (Date)

Name: Dave McCauley

Title: Chief Information Security Officer

4) **Chief Privacy Officer**

Robert B. Naylor (Signature) 3/5/10 (Date)

Name: Robert Naylor

Title: Chief Information Officer/Chief Privacy Officer