

**U.S. Securities and Exchange Commission**

---

Supplier Diversity Business Management System (SDBMS)  
**PRIVACY IMPACT ASSESSMENT (PIA)**



**May 23, 2019**

**Office of Minority and Women Inclusion**

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

### Section 1: System Overview

#### 1.1 Name of Project or System

Supplier Diversity Business Management System (SDBMS)

#### 1.2 Is the system internally or externally hosted?

- Externally Hosted (Contractor or other agency/organization)      Salesforce.com

#### 1.3 Reason for completing PIA

- New project or system

#### 1.4 Does the system or program employ any of the following technologies?

- Cloud Computing Services

### Section 2: Authority and Purpose of Collection

#### 2.1 Describe the project and its purpose or function in the SEC's IT environment

The Securities and Exchange Commission is required under Section 342 of the Dodd-Frank Wall Street and Reform Act to develop standards and processes for ensuring the fair inclusion of women-owned and minority-owned businesses in all of the Commission's business activities. To help implement this requirement, the Office of Minority and Women Inclusion (OMWI) maintains an electronic Supplier Diversity Business Management System (SDBMS) to collect up-to-date business information and capabilities statements from diverse suppliers interested in doing business with the Commission. SDBMS is a web-based application and allows the Commission to (1) learn about a potential supplier's interest in the Commission's contracting opportunities, (2) communicate with interested suppliers when opportunities arise, and (3) gather information on vendors and supplier diversity program activities to guide initiatives and facilitate Congressionally-mandated reporting on the Commission's contract awards. Information in the system primarily consists of company profiles with basic contract information and the capabilities of diverse businesses interested in contracting with the SEC. This information allows the Commission to update and more effectively manage its current internal repository. It also allows the Commission to measure the effectiveness of its technical assistance and outreach efforts, and target areas where additional program efforts are necessary.

The process flow for the OMWI SDBMS application is as follows:

1. A vendor may request access to SDBMS by (1) accessing SDBMS self-registry public facing site from OMWI's sec.gov landing page or (2) a SEC user can create a record for the vendor.
2. If the vendor accesses the vendor self-registry portal, the vendor will be required to fill out the new vendor form which contains basic contact and business information to be reviewed by a SEC user and approved. If the SEC user approves the request, the vendor will receive an email with a link and username granting them access to SDBMS.
3. If an SEC user creates a record, they would enable the vendor to login as a customer community user, which sends out an invite to the contact. The vendor would then be able to register using the link provided. Once the vendor is logged in, they will be required to fill out the necessary contact information and will be able to upload necessary documents to the notes and attachments.

All collections of information are voluntary. Internal users will be authenticated through single-sign-on (SSO) authentication with Active Directory. External users (i.e., vendors) access their customer portal outside of the SEC network via a separate URL and will be authenticated using a unique username and password.

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

### 2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

15 U.S.C. 77a et seq., 78a et seq., 80a-1 et seq., and 80b-1 et seq.

### 2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

No

### 2.4 Do you retrieve data in the system by using a personal identifier?

Yes, there is an existing SORN

Typically, information is retrieved by non-personal identifiers which include company name, business classification, or the North American Industry Classification System (NAICS) code. In limited instances where an individual's name is the vendor, the SEC will retrieve data using the individual's personal name. SORN SEC-56 Mailing, Contact and Other Lists will cover this retrieval.

### 2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

Yes

The following form is used to collect information related to vendors seeking to do business with the SEC

- OMB 3235-0724, Office of Minority and Women Inclusion (OMWI) Supplier Management System (expires: July 31, 2021)

### 2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

There is a risk that unauthorized users may view stored information within the system or use the information for reasons that are inconsistent with the original purpose for which the information was collected. To mitigate this risk, access is limited to those with a need to know and the information is limited to that which is necessary to perform job functions based upon pre-defined user roles and permissions. Approved users are trained on the proper safeguarding and handling of PII and complete annual privacy and security training.

## Section 3: Data Collection, Minimization, and Retention

### 3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

The system does not collect, maintain, use, or disseminate information about individuals.

#### Identifying Numbers

- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Social Security Number | <input type="checkbox"/> Alien Registration      | <input type="checkbox"/> Financial Accounts     |
| <input type="checkbox"/> Taxpayer ID            | <input type="checkbox"/> Driver's License Number | <input type="checkbox"/> Financial Transactions |
| <input type="checkbox"/> Employee ID            | <input type="checkbox"/> Passport Information    | <input type="checkbox"/> Vehicle Identifiers    |
| <input type="checkbox"/> File/Case ID           | <input type="checkbox"/> Credit Card Number      | <input type="checkbox"/> Employer ID            |
| <input type="checkbox"/> Other:                 |  |   |

#### General Personal Data

- |  |  |  |
|--|--|--|
| <input checked="" type="checkbox"/> Name           | <input type="checkbox"/> Date of Birth     | <input type="checkbox"/> Marriage Records      |
| <input type="checkbox"/> Maiden Name               | <input type="checkbox"/> Place of Birth    | <input type="checkbox"/> Financial Information |
| <input type="checkbox"/> Alias                     | <input type="checkbox"/> Home Address      | <input type="checkbox"/> Medical Information   |
| <input type="checkbox"/> Gender                    | <input type="checkbox"/> Telephone Number  | <input type="checkbox"/> Military Service      |
| <input type="checkbox"/> Age                       | <input type="checkbox"/> Email Address     | <input type="checkbox"/> Mother's Maiden Name  |
| <input type="checkbox"/> Race/Ethnicity            | <input type="checkbox"/> Education Records | <input type="checkbox"/> Health Plan Numbers   |
| <input type="checkbox"/> Civil or Criminal History | <input type="checkbox"/> Zip Code          |  |
| <input type="checkbox"/> Other:                    |  |  |

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

### Work-Related Data

- |  |  |  |
|--|--|--|
| <input type="checkbox"/> Occupation  | <input checked="" type="checkbox"/> Telephone Number | <input type="checkbox"/> Salary              |
| <input type="checkbox"/> Job Title   | <input checked="" type="checkbox"/> Email Address    | <input type="checkbox"/> Work History        |
| <input checked="" type="checkbox"/> Work Address                                 | <input type="checkbox"/> Certificate/License Number  | <input type="checkbox"/> Business Associates |
| <input type="checkbox"/> PIV Card Information                                    | <input type="checkbox"/> Fax Number                  |  |
| <input checked="" type="checkbox"/> Other: Business name and business NAICS code |  |  |

### Distinguishing Features/Biometrics

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Fingerprints    | <input type="checkbox"/> Photographs      | <input type="checkbox"/> Genetic Information |
| <input type="checkbox"/> Voice Recording | <input type="checkbox"/> Video Recordings | <input type="checkbox"/> Voice Signature     |
| <input type="checkbox"/> Other:          |   |  |

### System Administration/Audit Data

- |  |   |  |
|--|---|--|
| <input checked="" type="checkbox"/> User ID  | <input checked="" type="checkbox"/> Date/Time of Access | <input type="checkbox"/> ID Files Accessed |
| <input type="checkbox"/> IP Address  | <input type="checkbox"/> Queries Ran                    | <input type="checkbox"/> Contents of Files |
| <input type="checkbox"/> Other: User ID and Date/Time of Access are collected on internal users as part of an audit trail. |   |  |

### 3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

The data will be collected and used to: source diverse vendors for market research purposes, generate tailored vendor lists, track vendor outreach and communications (including supplier diversity initiatives), and track metrics/generate reports. This information allows the Commission to update and more effectively manage its current internal repository. It also allows the Commission to measure the effectiveness of its technical assistance and outreach efforts, and target areas where additional program efforts are necessary.

### 3.3 Whose information may be collected, used, shared, or maintained by the system?

- SEC Employees  
Purpose: User ID and date/time of access are collected on SEC employees for authentication and auditing purposes.
- SEC Federal Contractors  
Purpose: User ID and date/time of access are collected on SEC contractors for authentication and auditing purposes.
- Members of the Public  
Purpose: Basic contact information (name, telephone number, email address) is collected from vendor point of contacts (POC) and used to collect up-to-date business information and capabilities statements from diverse suppliers interested in doing business with the Commission.

### 3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

The PII from the system will not be used for testing, training and/or research efforts.

### 3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

- Yes  
The records are retained for 10 years under OMWI's retention schedule (record schedule DAA-0266-2016-0011-0002).

### 3.6 What are the procedures for identification and disposition at the end of the retention period?

Functionality has been built into the system to flag the records once they reach the end of the retention period.

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

Only the “records manager” role (assigned to the OMWI records management liaison) has the ability to delete records. All records will be maintained until they become inactive, at which time they will be retired and/or destroyed in accordance with record schedules of the United States Securities and Exchange Commission as approved by the National Archives and Records Administration.

### 3.7 Will the system monitor members of the public, employees, and/or contractors?

N/A

### 3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The risk presented by the use of contact information is that the information may be used in ways outside the scope intended by the initial collection. Per the systems of record notice SEC-56 Mailing, Contact and Other Lists and the Privacy Act Statement given prior to collection, information collected is to be used for the purpose of gathering, tracking and processing of contact information.

## Section 4: Openness and Transparency

### 4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

Privacy Act Statement

System of Records Notice  
SEC-56 Mailing, Contact and Other Lists

Privacy Impact Assessment  
Date of Last Update: Current PIA

Web Privacy Policy  
The new vendor form links to the SEC’s web site privacy and security policy.

### 4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

There is a risk that an individual does not know that their information is being stored on a server not owned or controlled by the U.S. Government (Salesforce). This risk is mitigated by the contract binding Salesforce to adhere to the Privacy Act requirements regardless of the storage location of the content management system that contains PII. The applicable records must be used in accordance with the purposes stated in the SORN. SEC-56 as well as this PIA provides notice to the public about the SEC’s collection, use, dissemination, and storage of information.

## Section 5: Limits on Uses and Sharing of Information

### 5.1 What methods are used to analyze the data?

SDBMS does not participate in data mining activities. It does not make available new or previously unavailable information about an individual. No information will be analyzed to determine patterns and no action(s) will be taken against any individual based on data entered into the system.

### 5.2 Will internal organizations have access to the data?

Yes

Organizations: Data will be shared with the Office of Acquisitions, primarily through the small business

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

specialists, for purposes of conducting market research for potential procurements. Data may also be shared with contracting officer representatives (CORs) throughout the agency. Reports may be accessed directly by the few SEC-licensed holders (7 total).

### 5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

A privacy concern stemming from internal sharing includes accidental disclosure of information to individuals without a need to know. Accidental disclosure typically stems from inadequate document control (hard or electronic copy), inadequate PII and security training, or insufficient knowledge of roles, authorization and need to know policies. To mitigate these risks, SEC staff are trained annually on the safe handling and storage of PII. Strict access controls are implemented based on roles and responsibilities and a need to know. Furthermore, any sharing of information must align with the purpose of the initial collection as well as the SORN and the PAS provided at the time of collection.

### 5.4 Will external organizations have access to the data?

No

Organizations: SDBMS is hosted on Salesforce, but Salesforce staff will not have access to the data. Internal access to the SDBMS is restricted to SEC approved IP addresses assigned within Salesforce. The SEC data within Salesforce is segregated and separate from hardware supporting other customers. Salesforce prevents unauthorized and unintended information transfer via share system resources through strong logical access controls. Aggregate data on topics such as how many vendors the SEC met at a certain event, or how many small businesses the SEC maintains profiles on may be included in the annual report to Congress, but those reports will not contain PII on individuals.

### 5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

There is no risk to privacy from external sharing as PII is not shared with external organizations.

## Section 6: Data Quality and Integrity

### 6.1 Is the information collected directly from the individual or from another source?

Directly from the individual.

### 6.2 What methods will be used to collect the data?

Data is collected via a web form that was configured in Salesforce for OMWI. Vendors may express interest in being included in the SDBMS and provide their information to the SEC at an OMWI event. In this case, the vendor will be provided a username and access link that can then be used to create a password and access the vendor profile form to complete. Vendors may also request access to the web form via a self-registry portal located on OMWI's public webpage.

### 6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

The information is collected directly from individuals who volunteer the information and is assumed to be accurate. Vendors are emailed annual reminders to verify the accuracy of the information contained in their profile. All information received is presumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise.

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

---

### 6.4 Does the project or system process, or access, PII in any other SEC system?

No

### 6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is a privacy risk that SDBMS may contain inaccurate or outdated information. This risk is mitigated by collecting information directly from the individuals to whom it applies. This ensures that the information collected, maintained, and disseminated is accurate. There may also be a risk of over collection of information which may impact data integrity. This risk is mitigated by the fact that individuals are the initial source of the information collected. They have the ability to limit the information that they provide as well as correct any information that is erroneous, inaccurate, or irrelevant.

## Section 7: Individual Participation

### 7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Individuals are not required to provide contact information. However, if contact information is not provided, companies will not be placed on the list of vendors interested in doing business with the Commission. Additionally, when a vendor first completes a profile, there are instructions on how to remove company profiles from the approved vendor lists.

### 7.2 What procedures are in place to allow individuals to access their information?

Each vendor has a unique username and password and is able to access and update their basic profile at any time.

### 7.3 Can individuals amend information about themselves in the system? If so, how?

Each vendor has a unique username and password and is able to access and update their basic profile at any time.

### 7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

There is a risk that inaccurate information may be stored in a vendor profile. This risk is mitigated by the fact that vendors may correct their information at any time during which the SEC possesses and uses their information. Any risks associated with correction of information are thoroughly mitigated by the individual's ability to correct their information via the same process by which they submitted information.

## Section 8: Security

### 8.1 Has the system been authorized to process information?

Yes

SA&A Completion Date: 6/4/2018

Date of Authority to Operate (ATO) Expected or Granted: 6/15/2018

### 8.2 Identify individuals who will have access to the data in the project or system and state their respective roles.

Users

Roles: Each vendor (external user) only has access to his/her company profile to ensure the information is accurate and up to date.

Program Staff

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

Roles: OMWI Suppler Diversity staff and OA Small Business Specialists have access to the preliminary information tab in order to invite vendors to self-register and add contacts. They also have access to read, edit, and delete any vendor profile. They may view/edit customized reports and dashboards.

System Administrators

Roles: Administrative users will audit reports on user activity and grant user access to the system. They may create new users, revoke user access, reset user passwords, and change user permissions.

### 8.3 Can the system be accessed outside of a connected SEC network?

Yes

If yes, is secured authentication required?  No  Yes  Not Applicable

Is the session encrypted?  No  Yes  Not Applicable

### 8.4 How will the system be secured?

Access to the SDBMS application will be restricted to approved IP addresses assigned within Salesforce. Internal users login to the system via SSO authentication validating the user by AD credentials. External users, if granted access by an internal SEC user will be authenticated using their username and password and will only have access to their vendor profile information. User access and audit logs will be reviewed by the SEC SDBMS system admins on a regular basis to prevent unauthorized access to the application. All logged events will be accompanied by an event id, user id, timestamp, application generating event, and resource reference at a minimum. OIT Security will also perform regular vulnerability scanning of operating systems, web applications, and databases as part of SEC's continuous monitoring strategy.

Perimeter intrusion detection system (IDS), network devices, and hosts are in place within the Salesforce boundary to monitor inbound and outbound traffic. Salesforce has also implemented the ArcSight software at the platform level for log correlation, review, and alert generation. All the data and meta-data within Salesforces is encrypted. Salesforce Storage engineers use a passphrase to encrypt keys on the data domain devices at the platform level. Keys are stored on the devices and access is protected based on least privilege and separation of duties. Mechanisms are in place to protect the confidentiality and integrity of information at rest (data on secondary storage devices). PROD databases and Fileforce storage are backed up to disk using the storage back up tool Data Domain. Data domain encrypts data at rest using AES-256 via FIPS 140-2 validated encryption (certificate #1058)

The Salesforce external boundary is protected by firewalls, access control lists (ACLs), and IDS. In the event of a security incident or breach of customer data, Salesforce will email the system owner and the system administrator of the SEC SDBMS application as soon as the incident or breach is realized.

Salesforce operates using a cloud-based delivery model. Salesforce.com customer products are hosted and served from the Production network. The Production network is logically and physically separated from the corporate network. Customers connect over the Internet to their organization's instance of Salesforce hosted on Salesforce.com's Production network. Salesforce.com defines this as an "Org' or "Customer Org." When a customer submits an authentication request to Salesforce, several processes occur that are not visible to the user, but are essential to provide the requested access.

### 8.5 Does the project or system involve an online collection of personal data?

Yes

Public URL: <https://sdbms.secure.force.com/SelfRegister/>

### 8.6 Does the site have a posted privacy notice?

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

Yes

### 8.7 Does the project or system use web measurement and/or customization technologies?

Yes, but they do not collect PII

The application uses cookies, both persistent and session-based, to manage access and use of the application, including to assist in the provision of application features and functionality. The non-persistent cookie is used to manage secure application access and to ensure that users are only accessing information they are authorized to access. It contains randomly generated information for that session only. All cookies served when using the Salesforce application are first party Salesforce cookies and are not utilized for marketing or any other activity not related to delivering the service to the customer in accordance with the agreement between Salesforce and its customer.

### 8.8 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

There is a risk of unauthorized access. This privacy risk is mitigated by role-based security that ensures the appropriate access to data within the system. The system offers a complete set of administrative reports in addition to custom auditing that enable SEC system administrators to monitor data changes. Audit logs will be reviewed via the administrative dashboard. The system is also capable of creating snapshots of the auditing reports in order to maintain point in time information. Additionally, technical and programmatic design choices analyze any proposed changes in terms of their life-cycle processes (collection, use and disclosure, processing and retention and destruction) and the potential the changes may create for noncompliance with relevant statutes or regulations (the Privacy Act in particular) or for violations of the fair information practice principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed. The company's privacy policy and previous industry audits are available at <https://www.salesforce.com/company/privacy/>.

## Section 9: Accountability and Auditing

### 9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All users must complete mandatory training on SEC Privacy and Information Security Awareness, Protecting Nonpublic Information, and Records Management.

### 9.2 Does the system generate reports that contain information on individuals?

Yes

Company POC name and business address may be included in internal reports. The reports are saved to the OMWI internal shared drive. The application is secure and only approved SEC users can access and pull reports. All SEC users have taken mandatory agency privacy training.

### 9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

Yes

### 9.4 Does the system employ audit logging or event logging?

Yes

OMWI SDBMS admins and/or privileged users are able to keep an audit of edits/data changes and data deletions. Salesforce has embedded auditing capabilities within the application and are responsible for auditing

# Privacy Impact Assessment

## Supplier Diversity Business Management System (SDBMS)

---

at the platform level. Salesforce has incorporated logging capabilities to ensure user log and log -off (successful and unsuccessful) is recorded, system administration activities, modifications of privilege and access, application alerts and error messages. Salesforce administrators are also responsible for adjusting the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, and/or individuals based on law enforcement information, intelligence information or other credible sources of information.

All user actions within the system are logged in the setup-audit trail logs hosted on Salesforce and accessible only to the system administrators. The platform produces audit records for the SEC that contain sufficient information to at a minimum establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

### **9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?**

Access to the system is determined by the system owner or alternates based upon the role that the end user has within OMWI. The system does not allow for anonymous login. To gain access, a user must be authenticated. As such, the SEC is capable of monitoring change activity within the system. A system usage warning banner is used and forces internal uses to acknowledge SEC's system usage standards prior to accessing data within SDBMS. User permissions are set so that each vendor (external user) has access to his/her company profile only. All internal SEC users with contracting responsibilities are authorized to browse the vendor data contained in the application for market research purposes. SEC system administrators review and analyze SDBMS system specific Salesforce audit records on a weekly basis for inappropriate or unusual activities.

Additionally, the SA&A will be completed by the OIT security team. The monitoring, testing, and the evaluation of the security controls will ensure that the implemented controls continue to work properly. The technical controls will be documented in the system security plan. The testing of these controls will be documented in the security assessment.

### **9.6 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.**

The information is stored on a third party server (Salesforce) and presents a risk that the SEC maybe unable to access and audit SEC records to ensure compliance with access, use, and record retention requirements. This risk is mitigated by the requirement for Salesforces, as a FedRAMP certified system, to permit the SEC to perform manual or automated audits, scans, review, or other inspections of the vendor's IT environment being used to provide or facilitate services for the SEC.