U.S. Securities and Exchange Commission

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

September 19, 2023

Office of Minority and Women Inclusion

Section I: System Overview

1.1 Name of Project or System

Supplier Diversity Business Management System (SDBMS)

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally hosted (Contractor or other agency/organization): Salesforce cloud

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed:	5/23/2019
Last updated:	2/3/2023
Description of update:	The update to version 2.3.0.1 integrates Login.gov for external user login and implements a self-scheduler for the monthly Office of Minority and Women Inclusion (OMWI) Vendor Outreach Day sessions.

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

☐ Electronic Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☒ Cloud Computing Services

☐ www.sec.gov Web Portal

☐ None of the Above

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 (SEC) 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 SEC's business activities. To satisfy this requirement, Supplier Diversity Business Management System (SDBMS), used by OMWI, is a repository of information and capabilities statements from suppliers interested in doing business with the SEC. SDBMS allows OMWI to (1) learn about a potential supplier's interest in the SEC'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 SEC's contract awards. In addition, SDBMS allows OMWI to measure the effectiveness of its technical assistance and outreach efforts, and target areas where additional program efforts are necessary.

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

Section 342 (c) of the Dodd Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5452(c).
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 or collect Social Security numbers (SSNs)? *This includes truncated SSNs.*

☒ No

☐ Yes
If yes, provide the purpose of collection:
If yes, provide the legal authority:

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

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN
SORN SEC-26 Mailing, Contact and Other Lists

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

☐ No
☒ Yes
Information related to vendors seeking to do business with the SEC is collected on form OMB 3235-0724, Office of Minority and Women Inclusion (OMWI) Supplier Management System (expires: September 30, 2024)

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

There is 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 authorized system users with a need to know and information accessed is limited to that which is necessary to perform job functions based upon pre-defined user roles and permissions.

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

☐ Social Security Number
☐ Taxpayer ID
☐ Employee ID
☐ File/Case ID
☒ Other: SAM.gov number
☐ Alien Registration
☐ Driver's License Number
☐ Passport Information
☐ Credit Card Number
☐ Financial Accounts
☐ Financial Transactions
☐ Vehicle Identifiers
☐ Employer ID

General Personal Data

☒ Name
☐ Maiden Name
☐ Alias
☐ Gender
☐ Age
☐ Race/Ethnicity
☐ Civil or Criminal History
☐ Other:
☐ Date of Birth
☐ Place of Birth
☐ Home Address
☐ Telephone Number
☐ Email Address
☐ Education Records
☐ Zip Code
☐ Marriage Records
☐ Financial Information
☐ Medical Information
☐ Military Service
☐ Mother's Maiden Name
☐ Health Plan Numbers

Work-Related Data

☐ Occupation
☐ Job Title
☒ Telephone Number
☒ Email Address
☐ Salary
☐ Work History

☒ Work Address
☐ PIV Card Information
☐ Certificate/License Number
☐ Fax Number
☐ Business Associates
☒ Other: Business name, business address, business telephone number, business email address and business North American Industry Classification System (NAICS) code

Distinguishing Features/Biometrics

☐ Fingerprints
☐ Voice Recording/Signature
☐ Other:
☐ Photographs
☐ Video Recordings
☐ Genetic Information

System Administration/Audit Data

☒ User ID
☐ IP Address
☐ Other:
☒ Date/Time of Access
☒ Queries Run
☐ ID Files Accessed
☐ Contents of Files

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

PII is collected and used to maintain current contact information for vendor information stored in the SDBMS repository.

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

☒ SEC Employees
Purpose: SEC employee user id and date/time of access are collected for authentication and auditing purposes.
☒ SEC Federal Contractors
Purpose: Contractor user id and date/time of access are collected for authentication and auditing purposes.
☐ Interns
Purpose:
☐ Members of the Public
Purpose:
☐ Employee Family Members
Purpose:
☐ Former Employees
Purpose:
☐ Job Applicants
Purpose:
☒ Vendors
Purpose: Vendor contact information and capabilities statements are collected.
☐ Other:
Purpose:

3.4 What mechanisms are in place to minimize the use of PII for testing, training, and research efforts?

PII stored in SDMS is not used for testing, training and/or research efforts.

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

☐ No.

☒ Yes.
The records are retained for ten years in accordance with OMWI retention schedule DAA-0266-2016-0011-0002.

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

Records in SDBMS are maintained until they become inactive, at which time they are retired and/or destroyed in accordance with the retention scheduled identified in section 3.5. The system has the capability to flag records that have reached the end of the ten-year retention period. Only the OMWI Records Management Liaison, assigned the "records manager" role, can delete records from the system at the end of the retention period.

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

☒ N/A
☐ Members of the Public
Purpose:
☐ Employees
Purpose:
☐ Contractors
Purpose:

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

The risk to privacy is minimal because the type of information collected is vendor work contact information. Access control is implemented to limit access to information collected to only authorized SBMS users.

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-26 Mailing, Contact and Other Lists
☒ Privacy Impact Assessment
Date of Last
Update:5/23/2019
☒ Web Privacy Policy

☐ Other notice:

☐ Notice was not provided

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

The risk to privacy regarding notice provided is minimal because adequate notice is provided as identified in section 4.1.

Section 5: Limits on Uses and Sharing of Information

5.1 What types of methods are used to analyze the data?

Information collected by the system is not analyzed.

5.2 Will internal organizations have access to the data?

☐ No

☒ Yes

Organizations: Data is shared with the Office of Acquisitions (OA) to conducting market research for potential procurements.

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

The privacy risk associated with internal sharing is inadvertent disclosure of information. This risk is mitigated by encrypting data and employing access control to restrict access to only information that was entered in the system by an authorized user.

5.4 Will external organizations have access to the data?

☒ No

☐ Yes

Organizations:

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 because 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 (vendor)

☐ Other source(s): .

6.2 What methods will be used to collect the data?

Vendors may provide information via a self-registry portal located on OMWI's public webpage. Also, they may express interest in being included in the SDBMS and provide information to the SEC at an OMWI event. In this case, the vendor is given an access link to create a password to access and complete the vendor profile form in SDBMS.

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

Information collected is assumed to be accurate. Vendors are emailed annually as a reminder to verify the accuracy of the information contained in their profile.

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

☒ No
☐ Yes.
System(s):

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 privacy risk that SDBMS may contain inaccurate or outdated information. This risk is minimized because information is collected from the vendor and assumed to be accurate. Vendors are contacted annually via email to verify accuracy of their information in the system.

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.

Vendors may consent, decline, or opt out of providing information in SDBMS.

7.2 What procedures will allow individuals to access their information?

Individuals seeking notification of and access to any record contained in this system of records may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-2736.

In addition, each vendor has a unique username and password and may access their basic profile information.

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

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549-2736.

In addition, each vendor has a unique username and password and may update their basic profile information. If the vendor has a change in staff, they must manually email OMWI@sec.gov for the System Administrator to deactivate the old account.

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

Privacy risk related to participation and redress is minimal because vendor participation in information collection is voluntary and any information collected may be accessed for amendment as described in section 7.3.

Section 8: Security

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

☐ No
☒ Yes

If yes, is secured authentication required?	☐ No	☒ Yes	☐ Not Applicable
Is the session encrypted?	☐ No	☒ Yes	☐ Not Applicable

8.2 Does the site have a posted privacy notice?

☐ No
☒ Yes
☐ N/A

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

☒ No
☐ Yes but they do not collect PII
☐ Yes and they collect PII

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system or project.

All SEC staff and contractors receive initial and annual privacy awareness training, which outline the roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security responsibilities and how to fulfill them.

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

☐ No
☒ 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?

☐ No
☒ Yes
☐ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ 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 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 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Residual risk related to access of information in SDBMS is minimal due to secure authentication of SEC users and vendors, access control, and encryption of data in transit and at rest.