GENERAL SERVICES ADMINISTRATION

[Notice-ID-2023-04; Docket No.2023-0002; Sequence No. 24]

Privacy Act of 1974; Notice of a New System of Records

AGENCY: Office of the Chief Privacy Officer, General Services Administration (GSA).

ACTION: Notice.

SUMMARY: GSA seeks to establish a new system of records for the Federal Service Desk (FSD) Program. The purpose of the system of records is to collect contact information, including usernames, email addresses and phone numbers, to support users of Integrated Award Environment (IAE) applications.

DATES: This system of records will go into effect without further notice on **[INSERT DATE 30 DAYS AFTER FEDERAL REGISTER PUBLICATION]** unless otherwise revised pursuant to comments received.

ADDRESSES: You may submit comments via email to the GSA Privacy Act Officer: *gsa.privacyact@gsa.gov*, or mail to the Privacy Office (IDE), GSA, 1800 F Street NW, Washington, DC 20405.

FOR FURTHER INFORMATION CONTACT: Richard Speidel, Chief Privacy Officer, GSA, by email at *gsa.privacyact@gsa.gov* or by phone at 202-969-5830.

SUPPLEMENTARY INFORMATION:

SYSTEM NAME AND NUMBER: GSA/FSD-1.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: GSA Federal Acquisition Service (FAS) is the owner and is responsible for the system. The system is hosted, operated, and maintained by contractors. Records are maintained in an electronic form on a Software as a Service (SaaS) platform, within the United States. Contact the system manager for additional information.

SYSTEM MANAGER(S): Salomeh Ghorbani, Acting Director Outreach and Stakeholder Engagement for the IAE Program Management Office, GSA, FAS, 1800 F Street, Washington, DC 20405.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204, 2 CFR, Subtitle A, Chapter I, and Part 25, and 40 U.S.C. 121(c).

PURPOSE(S) OF THE SYSTEM: The primary purpose of the FSD is to provide services to support users of current and future IAE applications. This support assists users in all Department of Defense and Civilian Departments and Agencies in the Federal Government, as well as all other users of the IAE.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Any entity to bid on and get paid for federal contracts or to receive federal funds. These include for-profit businesses, nonprofits, government contractors, government subcontractors, state governments, and local municipalities.

CATEGORIES OF RECORDS IN THE SYSTEM: The system collects necessary information from individuals and entities seeking to do business with the U.S Government. The data elements collected include full name, email address, and phone number.

RECORD SOURCE CATEGORIES: Information is obtained from individuals and entities seeking to do business with the U.S Government.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. By contracting officers and other Federal, state, local or tribal government employees involved in procuring goods and services with federal funds or administering Federal financial assistance programs or benefits to determine a party's eligibility status to participate in Federal procurement and non-procurement programs.

b. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law,

rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations.

c. To the Department of Justice (DOJ) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) GSA or any component thereof, or (b) any employee of GSA in his/her official capacity, or (c) any employee of GSA in his/her individual capacity where DOJ or GSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and GSA determines that the records are both relevant and necessary to the litigation.

d. To a court in connection with any litigation or settlement discussions regarding claims by or against GSA, to the extent that GSA determines the disclosure of the information is relevant and necessary to the litigation or discussions.

e. To an appeal, grievance, hearing, or complaints examiner; an equal employment opportunity investigator, arbitrator, or mediator; and an exclusive representative or other person authorized to investigate or settle a grievance, complaint, or appeal filed by an individual who is the subject of the record.

f. To the National Archives and Records Administration (NARA) for records management purposes.

g. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) in accordance with their responsibilities for evaluating federal programs.

h. To a Member of Congress or his or her staff on behalf of and at the request of the individual who is the subject of the record.

i. To another federal agency or federal entity, when GSA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

j. To appropriate agencies, entities, and persons when (1) GSA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) GSA has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or

another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

k. To agencies, to compare such records to other agencies' systems of records or to non-Federal records, in coordination with an Office of Inspector General (OIG) in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: All records are stored in a secure data center. PII is encrypted in transit, encrypted at rest, and not viewable by other users.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

FSD manages system and data access through role-based access controls. GSA requires all FSD personnel supporting the system to undergo background investigations and signing of Rules of Behavior. Non-FSD personnel (i.e., customer users) are required to authenticate through Login.gov when accessing FSD for ticket status or creation and are limited by system restrictions to only viewing and adding comments to their own tickets.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: System records are retained and disposed in accordance with GSA records maintenance and disposition schedules and 1820.2 CIO GSA Records Management Program, the requirements of the Recovery Board, and the National Archives and Records Administration (NARA).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: System records are safeguarded in accordance with the requirements of the Privacy Act, the Computer Security Act, and the FSD Security Plan. System roles are assigned with specific permissions to allow or prevent accessing certain information. Technical, administrative, and personnel security measures are implemented to ensure confidentiality and integrity of the system data that is stored, processed, and transmitted, including password protection and other appropriate security measures.

RECORD ACCESS PROCEDURES: Requests for access to records should be directed to the system manager. Individuals seeking access to their records in this system of records may submit a request by following the instructions provided in 41 CFR part 105-64.2.

CONTESTING RECORD PROCEDURES: Individuals wishing to contest the content of records about themselves contained in this system of records should contact the system manager at the address above. See 41 CFR part 105-64.4 for full

details on what to include in a Privacy Act amendment request.

NOTIFICATION PROCEDURES: Individuals seeking notification of any records about themselves contained in this system of records should contact the system manager at the address above. Follow the procedures on accessing records in 41 CFR part 105-64.2 to request such notification.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None

HISTORY: N/A

Richard Speidel,

Chief Privacy Officer,

Office of the Deputy Chief Information Officer,

General Services Administration.

[FR Doc. 2023-19454 Filed: 9/8/2023 8:45 am; Publication Date: 9/11/2023]