than 20 days after Respondents consummate ICE's acquisition of Black Knight. The Order to Maintain Assets requires Respondents to maintain the viability of the divestiture assets until the divestitures are complete.

The D&O contains additional provisions designed to ensure the effectiveness of this relief. For example, the D&O requires Respondents to provide Constellation with transition assistance as it integrates the acquired assets to enable Constellation to operate the divested businesses similarly to how they were operated by Black Knight. The D&O also requires Respondents to obtain all third-party and governmental consents necessary to effectuate the divestitures.

To help Constellation succeed in operating the divested assets, the D&O further requires Respondents for one year to facilitate Constellation's hiring of certain employees of the Black Knight divisions responsible for the Empower LOS and Optimal Blue, to the extent they were not already included in the divestitures. The D&O similarly prohibits Respondents from soliciting Constellation employees who came from Black Knight to work in the divested businesses for two years. It also prohibits Respondents from enforcing any noncompete or non-solicit provision or agreement against any employee who seeks or obtains a position in the divested businesses during the term of the D&O.

The D&O protects the confidential information of the divested Black Knight divisions as well as confidential information that Respondents may learn from Constellation in the course of providing transition services. These safeguards include limiting the purposes for which Respondents may use such confidential information and the employees to whom the information may be disclosed. The D&O facilitates the execution of NDAs by Black Knight employees who possess confidential information and who will remain with Respondents post-divestiture, and it prevents Respondents from allowing any such employees who decline to sign an NDA from working on an ICE LOS or PPE.

Black Knight and Constellation have agreed that Black Knight will finance a portion of Constellation's purchase price of Optimal Blue via a promissory note. In order to ensure that Respondents do not have a continuing entanglement with Constellation based on the promissory note, the D&O provides that the Commission will appoint a seller note trustee no later than one day after the divestiture closes. Not later than ten days after the Commission appoints the trustee, Respondents must transfer their rights, title, and interest in the promissory note to the trustee. The trustee will sell the note to a third party within six months of the divestiture.

The D&O requires Respondents to obtain prior approval from the Commission before reacquiring any divested assets or acquiring an interest in any business that owns or sells an LOS for ten years. The D&O also requires Respondents to provide the Commission with prior notice before acquiring an interest in any business that owns or sells a PPE for ten years. The D&O requires Constellation to obtain prior approval from the Commission before selling any of the divested assets for three years after the divestitures and for another seven years if the acquiring firm operates an LOS or PPE. Finally, the D&O provides for the appointment of an independent monitor to oversee compliance with the D&O's requirements.

The purpose of this analysis is to facilitate public comment on the Consent Agreement, and the Commission does not intend this analysis to constitute an official interpretation of the Consent Agreement or the D&O or modify their terms in any way.

By direction of the Commission.

**April J. Tabor,**

*Secretary.*

[FR Doc. 2023–19534 Filed 9–8–23; 8:45 am]

**BILLING CODE 6750–01–P**

## 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 October 11, 2023 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 9–8–23; 8:45 am]

**BILLING CODE P**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Centers for Medicare and Medicaid Services

### Privacy Act of 1974; Matching Program

**AGENCY:** Centers for Medicare & Medicaid Services, Department of Health and Human Services.

**ACTION:** Notice of a new matching program.

**SUMMARY:** In accordance with the Privacy Act of 1974, as amended, the Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) is providing notice of the re-establishment of a matching program between CMS and the Department of Veterans Affairs (VA), Veterans Health Administration (VHA), ''Verification of Eligibility for Minimum Essential Coverage Under the Patient Protection and Affordable Care Act Through a Veterans Health Administration Plan.''

**DATES:** The deadline for comments on this notice is October 11, 2023. The re-established matching program will commence not sooner than 30 days after publication of this notice, provided no comments are received that warrant a change to this notice. The matching program will be conducted for an initial term of 18 months (from approximately November 2, 2023 to May 1, 2025) and within 3 months of expiration may be renewed for one additional year if the parties make no change to the matching program and certify that the program has been conducted in compliance with the matching agreement.

**ADDRESSES:** Interested parties may submit written comments on the new matching program to the CMS Privacy Act Officer by mail at: Division of Security, Privacy Policy & Governance, Information Security & Privacy Group, Office of Information Technology, Centers for Medicare & Medicaid Services, Location: N1–14–56, 7500 Security Blvd., Baltimore, MD 21244–1850, or by email at *Barbara.Demopulos@cms.hhs.gov.*

**FOR FURTHER INFORMATION CONTACT:** If you have questions about the matching program, you may contact Anne Pesto, Senior Advisor, Marketplace Eligibility and Enrollment Group, Center for Consumer Information and Insurance Oversight, Centers for Medicare & Medicaid Services, at 443–844–9966, by email at *anne.pesto@cms.hhs.gov,* or by mail at 7500 Security Blvd., Baltimore, MD 21244.

**SUPPLEMENTARY INFORMATION:** The Privacy Act of 1974, as amended (5 U.S.C. 552a) provides certain protections for individuals applying for and receiving federal benefits. The law governs the use of computer matching by federal agencies when records in a system of records (meaning, federal agency records about individuals retrieved by name or other personal identifier) are matched with records of other federal or non-federal agencies. The Privacy Act requires agencies involved in a matching program to:

1. Enter into a written agreement, which must be prepared in accordance with the Privacy Act, approved by the Data Integrity Board of each source and recipient federal agency, provided to Congress and the Office of Management and Budget (OMB), and made available to the public, as required by 5 U.S.C. 552a(o), (u)(3)(A), and (u)(4).

2. Notify the individuals whose information will be used in the matching program that the information they provide is subject to verification through matching, as required by 5 U.S.C. 552a(o)(1)(D).

3. Verify match findings before suspending, terminating, reducing, or making a final denial of an individual's benefits or payments or taking other adverse action against the individual, as required by 5 U.S.C. 552a(p).

4. Report the matching program to Congress and the OMB, in advance and annually, as required by 5 U.S.C. 552a(o)(2)(A)(i), (r), and (u)(3)(D).

5. Publish advance notice of the matching program in the **Federal Register** as required by 5 U.S.C. 552a(e)(12).

This matching program meets these requirements.

**Barbara Demopulos,**

*Privacy Act Officer, Division of Security, Privacy Policy and Governance, Office of Information Technology, Centers for Medicare & Medicaid Services.*

#### Participating Agencies

The Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS) is the recipient agency, and the Department of Veterans Affairs (VA), Veterans Health Administration (VHA) is the source agency.

#### Authority for Conducting the Matching Program

The statutory authority for the matching program is 42 U.S.C. 18001 *et seq.*

#### Purpose(s)

The purpose of the matching program is to assist CMS in determining individuals' eligibility for financial assistance in paying for private health insurance coverage. In this matching program, VHA provides CMS with data when a state administering entity (AE) requests it and VHA is authorized to release it, verifying whether an individual who is applying for or is enrolled in private health insurance coverage under a qualified health plan through a federally-facilitated health insurance exchange or state-based exchange is eligible for coverage under a VHA health plan. CMS makes the data provided by VHA available to the requesting AE through a data services hub to use in determining the applicant's or enrollee's eligibility for financial assistance (including an advance tax credit and cost-sharing reduction, which are types of insurance affordability programs) in paying for private health insurance coverage. VHA health plans provide minimum essential coverage, and eligibility for such plans precludes eligibility for financial assistance in paying for private coverage. The data provided by VHA under this matching program will be used by CMS and AEs to authenticate each enrollee's identity, determine the enrollee's eligibility for financial assistance, and determine the amount of the financial assistance.

#### Categories of Individuals

The categories of individuals whose information will be used in the matching program are Veterans whose records at VHA match identifying data provided to VHA by CMS (submitted by AEs) about individuals who are applying for or are enrolled in private insurance coverage under a qualified health plan through a federally-facilitated health insurance exchange or state-based exchange.

#### Categories of Records

The categories of records used in the matching program are identity records and minimum essential coverage period records, consisting of the following data elements:

Data provided by CMS to VHA:

a. first name (required)
b. middle name/initial (if provided by applicant)
c. surname (applicant's last name) (required)