This document is scheduled to be published in the Federal Register on 2026-11-20 and available online at https://www.federalregister.gov/d/2026-23620, and on https://govinfo.gov

732-01-P

FEDERAL MEDIATION AND CONCILIATION SERVICE

Privacy Act of 1974; System of Records

AGENCY: Federal Mediation and Conciliation Service.

ACTION: Notice of a new system of records.

SUMMARY: GO.gov, which is developed by the General Service Administration (GSA), is a fully modernized, cloud-based travel and expense management platform tailored to meet the evolving needs of federal civilian agencies and their travelers. FMCS employees and contractors use Go.gov to plan, authorize, arrange, process and mange official FMCS travel; to maintain records on individual who are current FMCS employees on travel and individuals being provided travel by the Government; to obtain travel authorizations; to prepare and submit local travel vouchers; to generate travel expense reports; and to enable travel agents who are under contract to the Federal government to issue and account for travel provided by individuals.

DATES: This system of records will be effective without further notice on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless otherwise revised pursuant to comments received. New routine uses will be effective on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may send comments, identified by docket number FMCS-2026-0199, by any of the following methods:

- Federal eRulemaking Portal at https://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Office of General Counsel, 250 E Street, SW, Washington, DC 20427.

- Fax: (202) 606-5444.

Instructions: All comments must be received by the end of the comment period for them to be considered. All comments and other submissions received generally will be posted on the internet at regulations.gov as they are received, without change, including any personal information provided. However, FMCS retains discretion to redact personal or sensitive information, including but not limited to personal or sensitive information pertaining to third parties, where appropriate.

A summary of this rule may be found in the docket for this rulemaking at www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Anna Davis, General Counsel, at adavis@fmcs.gov.

SUPPLEMENTARY INFORMATION: This describes a new system for FMCS employees on travel and individuals being provided travel by the Government. GSA, however, proposes to modify a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a, to make technical changes to GSA/GOVT-4 consistent with the template laid out in OMB Circular No. A-108. Accordingly, GSA has made technical corrections and non-substantive language revisions to the following sections: "Policies and Practices for Storage of Records", "Policies and Practices for Retrieval of Records", "Policies and Practices for Retention and Disposal of Records", "Administrative, Technical and Physical Safeguards", "Record Access Procedures", "Contesting Record Procedures", and "Notification Procedures." GSA has also created the following new sections: "Security Classification" and "History."

SYSTEM NAME AND NUMBER: FMCS-00014 Go.gov.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: System records for *GO.gov,* — the next-generation federal

travel and expense system that replaced ETSNext — are primarily stored at the Travel and Expense (T&E) service provider, SAP Concur, a FedRAMP-authorized cloud service provider, under contract with GSA's Federal Acquisition Service (FAS).) In addition, records will be stored by Travel Management Companies (TMCs) available on the Multiple Award Schedule, 561510.

SYSTEM MANAGER(S): Director, Office of Travel, Employee Relocation, and Transportation Services (QMC), General Services Administration, 1800 F Street NW, Washington, DC 20405 and Financial Resources at FMCS, financialresources@fmcs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 5701-5739, 31 U.S.C. 3511, 3512, and 3523; and the Federal Travel Regulation, 41 CFR Chapters 300-304.

PURPOSE(S) OF THE SYSTEM: To plan, authorize, arrange, process and manage records on individuals who are current FMCS employees on travel and individuals being provided travel by the Government; to obtain travel authorization; to prepare and submit local travel vouchers; to generate travel expense reports; and to enable Travel Management Companies (TMCs) providing services under contract to the Federal Government (Multiple Award Schedule (MAS)) to issue reservations and air/rail tickets, lodging, and rental cars.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The system encompasses all FMCS employees or other individuals (e.g., witnesses) who are authorized to perform official travel, FMCS employees authorized to manage travel, FMCS employees authorized to approve travel/reimbursement, and individuals not employed (e, g., invitational traveler) by the Federal government being provided travel by the Federal Government.

CATEGORIES OF RECORDS IN THE SYSTEM: System records include a

traveler's profile containing: Full name of individual which matches the name on the form of ID used for travel (*e.g.,* driver's license, passport); employee identification number; travel personnel role; home and office telephone numbers; home address; home and office email addresses; emergency contact name and telephone number; entity name (*e.g.,* agency, financial institution, travel vendor), entity identifier, address, and telephone number; air travel preference; rental car identification number and car preference; hotel preference and room preference, current passport number, driver's license number, permanent resident card number, national identification number, and/or visa number(s); credit card numbers and related information; balance owed; bank account information needed for electronic funds transfer; frequent traveler/loyalty account information (*e.g.,* frequent flyer account numbers); date of birth; sex; medical information for a reasonable accommodation (*e.g.,* wheelchair); dietary restrictions; meal preference; redress number (number DHS assigns to passenger to promote resolution with previous watch list alerts); Known Traveler Number (passenger number DHS utilizes to facilitate passenger clearance *e.g.,* TSA Pre-Check, Global Entry); travel companion/attendee name; travel purpose; passenger name record (PNR); trip information (*e.g.,* destinations, reservation information; car rental pickup/dropoff, hotel reservation details); travel authorization/request information; travel claim (voucher/expense report) information (*e.g.,* expense receipts/amounts); monthly reports from travel agent(s) showing charges to individuals, balances, and other types of account analyses; and other official travel related information.

RECORD SOURCE CATEGORIES: Information in this system of records is provided by traveling FMCS employees by travel authorizations (request), travel voucher (expense report), credit card companies, and travel service providers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM,

INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

For any routine use noted in the GSA Privacy Act system of records notice applicable to this system, GSA/GOVT-4, or any successor system notice for this system. In addition, FMCS is generally permitted to disclose under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system to authorized entities, as is determined to be relevant and necessary, outside the FMCS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a) To another Federal agency, Travel Management Center (TMC), online booking tool (OBT) suppliers and the airlines that are required to support the DHS/TSA Secure Flight program. In this program, DHS/TSA assumes the function of conducting pre-flight comparisons of airline passenger information to Federal Government watch lists. In order to supply the appropriate information, these mentioned parties are responsible for obtaining new data fields consisting of personal information for date of birth, sex, redress number, and known traveler number. At this time, the redress number is optional, and the known traveler number is for future programs. They may be required to be stored in another phase of the Secure Flight program.

b) To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler profile information.

c) To a Federal agency employee, expert, consultant, or contractor while performing TDY travel, who is taking leave while on official travel, for purposes of tracking travel expenses that are the responsibility of the traveler and not the Federal Government, including, but not limited to, change fees, traveler personal itinerary information, etc.

d) To a Federal agency employee, expert, consultant, or contractor in tracking and providing assistance to provide technical support (e.g., helpdesk), or resolve a travel-related issue *e.g.,* changes when flights are cancelled.

e) To a credit card company for billing purposes, including collection of past due amounts.

f) To an expert, consultant, or contractor working on behalf of FMCS in the performance of a federal duty to which the information is relevant and as it pertains to travel of FMCS employees."

g) .To a Federal agency by the contractor in the form of itemized statements or invoices, and reports of all transactions, including refunds and adjustments to enable audits of charges to the Federal Government. This is related to interagency agreements (IAA) and the need to turn over documents related to performing under the IAA.

h) To Go.gov for billing and refund purposes.

i) To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule regulation or order where the record, either alone or in conjunction with other information creates an indication of a violation or potential violation of civil or criminal laws or regulations.

j) To the Government Accountability Office (GAO) for oversight purposes; to the Department of Justice (DOJ) to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or to the Office of Management and Budget (OMB) to obtain that office's advice regarding obligations under the Privacy Act.

k) To disclose information to the National Archives and Records Administration (NARA) or the General Services Administration in

records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

l) To a former employee of the Agency for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Agency regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Agency requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

m) To officials of labor organizations recognized under 5 U.S.C. Chapter 71 upon receipt of a formal request and in accordance with the conditions of 5 U.S.C. 7114 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

n) To disclose information to a Member of Congress or a congressional office in response to an inquiry made on behalf of, and at the request of, an individual who is the subject of the record.

o) To the Department of Justice, including Offices of the U.S. Attorneys; another Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body; another party in litigation before a court, adjudicative, or administrative body; or to a court, adjudicative, or administrative body. Such disclosure is permitted only when it is relevant and necessary to the litigation or proceeding, and one of the following is a party to the litigation or has an interest in such litigation:

1) FMCS, or any component thereof;
2) Any employee or former employee of FMCS in their official capacity;
3) Any employee or former employee of FMCS in their capacity where the Department of Justice or FMCS has agreed to represent the employee;
4) The United States, a Federal agency, or another party in litigation before a court, adjudicative, or administrative body, upon the FMCS General Counsel's approval, pursuant to 5 CFR part 295 or otherwise.

p) To any federal agency, organization, or person for the purpose of performing audit or oversight operations related to the operation of this system of records as authorized by law, but only information necessary and relevant to such audit or oversight function.

q) To appropriate agencies, entities, and persons when (1) FMCS suspects or has confirmed that there has been a breach of the system of records,·(2) FMCS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, FMCS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with FMCS’s efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

r) To another Federal agency or Federal entity, when FMCS 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

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Data entered into the system database by traveling FMCS individuals and/or FMCS staff through the Go.gov website is stored electronically in a database. Information is encrypted in transit and at rest. GO.gov records are managed under the General Record Schedule 1.1, item 010 Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. The records created under this schedule are retained for 6 fiscal years after completion of the transaction and all payments made on travel or arrangements. The detailed schedule can be found at: https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records kept by FMCS can be retrieved by full name of individual, Employee ID, DOB and email address. Records are retrieved in accordance with policies and practices issued by the National Archives and Records Administration (NARA) and must only be retrieved by authorized users, adhering to applicable laws, regulations and agency schedules.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records kept by FMCS are maintained in accordance with the General Records Retention Schedules issued by the National Archives and Records Administration (NARA) or an agency and NARA approved records disposition schedule.

- GRS 01.1/010 Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, And Accounting.

- Retention Instructions: Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.
- Legal Disposition Authority: DAA-GRS-2013-0003-0001 (GRS 01.1/010).
- Approved by NARA: 6/12/2014.

ADMINSTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: FMCS restricts access to FMCS personnel or contractors whose responsibilities require access. Records in the system are protected from unauthorized access and misuse through a combination of administrative, technical, and physical security measures. Administrative measures include, but are not limited to, policies that limit system access to individuals within an agency with a legitimate business need and regular review of security procedures and best practices to enhance security. Technical measures include, but are not limited to, system design that allows authorized system users access only to data for which they are responsible, required use of multifactor authentication, and use of encryption for data transfers. Physical security measures include, but are not limited to, the use of data centers which meet NIST requirements for storage of sensitive data.

RECORD ACCESS PROCEDURES: See § 1410 of the FMCS's rules of practice, 29 CFR 1410.3, Individual access requests. Individuals must provide the following information for

their records to be located and identified: (1) Full name, (2) Address, and (3) A specific description of the record content requested. Also, see https://www.fmcs.gov/privacy-policy/.

CONTESTING RECORDS PROCEDURES: See 29 CFR 1410.6, Requests for correction or amendment of records, on how to contest the content of any records. Privacy Act requests to amend or correct records may be submitted to the Privacy Office at privacy@fmcs.gov or via mail at Federal Mediation and Conciliation

Service, 250 E

Street, SW, Washington, DC 20427. Also, see https://www.fmcs.gov/privacy-policy/.

NOTIFICATION PROCEDURES: See 29 CFR 1410.3(a), Individual access requests.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Dated: November 17, 2026.

Anna Davis,

General Counsel and Performing the duties of Director.

[FR Doc. 2026-23620 Filed: 11/19/2026 8:45 am; Publication Date: 11/20/2026]