amended; 49 CFR 1.49; and DOT Order 1351.29A.

Nanda Narayanan Srinivasan,

Associate Administrator, Research and Program Development.

[FR Doc. 2024–10851 Filed 5–16–24; 8:45 am]

BILLING CODE 4910–59–P

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

[Docket No.: DOT–OST–2023–0136]

Privacy Act of 1974; System of Records

AGENCY: Federal Motor Carrier Safety Administration (FMCSA), Department of Transportation (DOT).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Transportation (DOT) proposes a new system of records titled ''DOT/FMCSA 014 Electronic Logging Device (ELD) Records''. This system of records is used to facilitate the retrieval, transfer, and collection of hours-of-service (HOS) data from electronic ELD files submitted by motor carriers and the review of HOS data by authorized safety officials. The system retrieves data recorded by a motor carrier's ELD via an ELD output file. Upon receipt of this ELD output file, the system analyzes the data, identifies instances of potential non-compliance, and notifies the authorized safety official of these instances. FMCSA maintains ELD data for use in investigations and enforcement actions and to determine compliance with HOS requirements. The primary purpose of the ELD system is to allow authorized safety officials to assess electronic ELD files rapidly and accurately at roadside and during reviews and safety audits to determine whether the driver is in compliance with the HOS regulations. The ELD system will also be used to assess whether ELDs meet certain technical specifications that are set forth in the HOS regulations. Additionally, the Agency may use ELD data internally to inform research efforts related to enforcement of safety regulations, including driving hours, as such research may ultimately improve compliance with HOS requirements.

DATES: Comments on the system will be accepted on or before 30 days from the date of publication of this notice. The system will be effective 30 days after publication of this notice. Routine uses will be effective at that time.

ADDRESSES: You may submit comments, identified by docket number OST-2023–0136 by one of the following methods:

- *Federal e-Rulemaking Portal: https://www.regulations.gov.*
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave. SE, West Building Ground Floor, Room W12–140, Washington, DC 20590–0001.
- *Hand Delivery or Courier:* West Building Ground Floor, Room W12–140, 1200 New Jersey Ave. SE, between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal holidays.

Instructions: You must include the agency name and docket number DOT–OST–2023–0136. All comments received will be posted without change to *https://www.regulations.gov,* including any personal information provided.

FOR FURTHER INFORMATION CONTACT: For general and privacy questions, please contact: Karyn Gorman, Departmental Chief Privacy Officer, Department of Transportation, S–83, Washington, DC 20590, Email: *privacy@dot.gov,* Tel. (202) 366–3140.

SUPPLEMENTARY INFORMATION:

Background

In accordance with the Privacy Act of 1974, the Department of Transportation is proposing a new system of records titled ''Department of Transportation (DOT)/Federal Motor Carrier Safety Administration (FMCSA) 014, Electronic Logging Device Records.'' This system will access hours-of-service (HOS) data via electronic logging device (ELD) files submitted by motor carriers and will allow authorized safety officials to assess these electronic ELD files rapidly and accurately at roadside and during reviews and safety audits to determine whether the driver is in compliance with the HOS regulations. This system will also assess whether ELDs meet certain technical specifications that are set forth in HOS regulations and support removals from a list of self-certified devices. See 49 CFR part 395 subpart B, app. A. Additionally, the Agency may use data from this system internally and/or in aggregated and anonymized form to inform research efforts related to enforcement of safety regulations, including driving hours, as such research may ultimately improve compliance with HOS requirements. For example, the use of ELD data in research related to operational testing of electronic, in-motion commercial motor vehicle (CMV) inspections may increase roadside inspection capacity and further facilitate enforcement of HOS requirements.

Section 32301(b) of the Commercial Motor Vehicle Safety Enhancement Act of 2012 (enacted as part of the Moving Ahead for Progress in the 21st Century Act (MAP–21)) codified at 49 U.S.C. 31137, mandated that the Secretary of Transportation adopt regulations requiring that CMVs, operated in interstate commerce by drivers required to maintain records of duty status (RODS), be equipped with ELDs. The statute also set forth specific provisions to be addressed by the regulations, including ELD design and performance standards and certification requirements. In addition, the statute addresses privacy protections and the use of ELD data, requiring that the regulations ensure that ELDs are not used to harass a CMV operator. On December 16, 2015, FMCSA, acting primarily under the authority of MAP–21 (and several concurrent statutory authorities), published a final rule, Electronic Logging Devices and Hours of Service Supporting Documents (80 FR 78292) requiring the use of ELDs for recording HOS information. Under the regulations, which were implemented on December 18, 2017, CMVs operated in interstate commerce, by drivers required to maintain RODS, must be equipped with ELDs. The regulations also establish ELD performance and design standards, require ELDs to be certified and registered with FMCSA, and address privacy protections for CMV operators. The ELD regulations are set forth in 49 CFR part 395, subpart B.

FMCSA's ELD system consists of the following components:

- Electronic Record of Duty Status (eRODS) HOS review tool
- ELD website and database
- ELD provider web service
- Enforcement ELD web service
- Enforcement ELD summary data web service

Electronic Record of Duty Status (eRODS) HOS review tool. eRODS is a software application installed on authorized safety officials' computers that is used to retrieve and display the information on an ELD output file. eRODS allows enforcement users to analyze a driver's HOS data and perform a roadside inspection or an investigation. There is also a web-based version of eRODS that consists of all the functionality included in the desktop version but is accessible via the ELD website described below. ELD devices used by motor carriers are required to support one of two options for providing an ELD file to FMCSA for analysis via the eRODS HOS review tool:

Option 1 is the telematics transfer method. ELD devices that utilize the telematics transfer method support transfer of ELD files to the FMCSA's ELD system via web services transfer or encrypted email transfer. With the web service transfer method, the ELD device sends the ELD file directly to FMCSA servers via a secure call to the ELD provider web service, which makes the ELD file available to eRODS. For the email transfer, the ELD device sends the data file via secure, encrypted email to FMCSA servers which process the email and make the ELD file available to eRODS.

Option 2 is local transfer, which consists of Bluetooth connection or USB transfer. The Bluetooth connection allows the motor carrier's ELD to use the safety official's internet connection to transfer the ELD file to the ELD provider web service. The USB transfer method uses the safety official's self-encrypting USB device to transfer the ELD file from the motor carrier's ELD device to the safety official's eRODS application. This is the only method that does not require internet connectivity.

ELD website and database. The ELD website and database is the centerpiece of FMCSA's ELD system. The website includes a section for each stakeholder. ELD vendors use the website to register their organization with FMCSA and to self-certify their devices' compliance with ELD regulations. ELD vendors also have access to tools necessary to build and test their interfaces with FMCSA. Motor carriers and drivers can access the ELD website to obtain information on the ELD Rule and other communications that educate them on the ELD process. They can also review the list of self-certified ELD devices. Enforcement users can access ELD policy and training information related to ELDs and can access web eRODS to review motor carrier HOS compliance. The FMCSA vendor vetting team also reviews ELD vendor submissions for completeness.

ELD provider web service. The ELD provider web service provides the means for a registered, self-certified ELD device to transfer, via web service or blue-tooth transfer options, an ELD file to FMCSA. During the self-certification process for an ELD device, the ELD vendor provides FMCSA with their public certificate and receives FMCSA's public certificate and additional information on building the connection between their ELD and FMCSA's ELD provider web service. Once the connection is established, the ELD can submit output files of a driver's HOS data to FMCSA via this service.

Enforcement ELD web service. The enforcement ELD web service is used to transfer the ELD files submitted to FMCSA to the safety official's eRODS HOS review tool. Both the desktop and web-based eRODS tools connect to this service. Files that are submitted via ELD provider web service, Bluetooth connection, or email can be accessed by enforcement via a connection to this service.

Enforcement ELD summary data web service. This service provides safety officials summary information derived from the contents of an ELD file that was submitted to the ELD system. This summary data enables safety officials to review indicators prompting further analysis and also allows implementation of a direct link to eRODS tool for HOS analysis. FMCSA's ELD system of records will also serve as a central repository of ELD information.

FMCSA has also included DOT General Routine Uses, to the extent they are compatible with the purposes of this System. As recognized by the Office of Management and Budget (OMB) in its Privacy Act Implementation Guidance and Responsibilities (65 FR 19746 (July 9, 1975)), the routine uses include proper and necessary uses of information in the system, even if such uses occur infrequently. FMCSA has included in this notice routine uses for disclosures to law enforcement when the record, on its face, indicates a violation of law, to DOJ for litigation purposes, or when necessary to investigate or respond to a breach or potential breach of this system or other agencies' systems. DOT may disclose to Federal, State, local, or foreign agency information relevant to law enforcement, litigation, and proceedings before any court or adjudicative or administrative body. OMB has long recognized that these types of routine uses are ''proper and necessary'' uses of information and qualify as compatible with agency systems (65 FR 19476, April 11, 2000).

In addition, OMB Memorandum M–17–12, directed agencies to include routine uses that will permit sharing of information when needed to investigate, respond to, and mitigate a breach of a Federal information system. DOT also has included routine uses that permit sharing with the National Archives and Records Administration when necessary for an inspection, to any Federal Government agency engaged in audit or oversight related to this system, or when DOT determines that the disclosure will detect, prevent, or mitigate terrorism activity. These types of disclosures are necessary and proper uses of information in this system because they further DOT's obligation to fulfill its records management and program management responsibilities by facilitating accountability to agencies charged with oversight in these areas, and DOT's obligation under the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108–456, and Executive Order 13388 (Oct. 25, 2005) to share information necessary and relevant to detect, prevent, disrupt, preempt, or mitigate the effects of terrorist activities against the territory, people, and interests of the United States.

Privacy Act

The Privacy Act (5 U.S.C. 552a) governs the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act extends rights and protections to individuals who are U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides a covered person with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the Electronic Logging Device System of Records. In accordance with *5 U.S.C. 552*a(r), DOT has provided a report of this system of records to the OMB and to Congress.

SYSTEM NAME AND NUMBER:

Department of Transportation (DOT)/ Federal Motor Carrier Safety Administration (FMCSA) 014 Electronic Logging Device (ELD) Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained in a FedRAMP-certified third-party cloud environment. The contracts are maintained by DOT at 1200 New Jersey Avenue SE, Washington, DC 20590.

SYSTEM MANAGER(S):

Division Chief, Enforcement Division, Office of Enforcement and Compliance, FMCSA, U.S. Department of

Transportation, 1200 New Jersey Avenue SE, Washington, DC 20590.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 32301(b) of the Commercial Motor Vehicle Safety Enhancement Act, enacted as part of the Moving Ahead for Progress in the 21st Century Act (Pub. L. 112–141, 126 Stat. 405, (July 6, 2012), codified at 49 U.S.C. 31137. (MAP–21); 49 CFR parts, 385, 386, 390, and 395.

PURPOSE(S) OF THE SYSTEM:

The purposes of the system are to (1) allow Federal and State law enforcement agencies to match an interstate CMV driver's name with his or her HOS record; (2) allow authorized safety officials to perform HOS compliance-assurance and enforcement functions for the purposes of using personal information to verify the time, date, and location for duty status changes of interstate CMV drivers to ensure that motor carriers and interstate drivers comply with applicable HOS regulations; (3) allow for assessment of particular ELD models and units to determine that they meet the technical specifications set forth in the HOS regulations; and (4) allow ELD data to inform research efforts related to safety regulations, including driving hours, to improve compliance with HOS requirements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals within this system include commercial motor vehicle CMV drivers.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in the system include the following information about CMV Drivers. Data elements marked with an asterisk ''*'' may be PII linked to ELD username or driver/co-driver name or license number.

- ELD username
- Driver's first name, last name
- Co-driver first name, last name (if there is a co-driver)
- Co-driver ELD username (if there is a co-driver)
- Driver's license number or commercial driver's license number
- State of license issuance*
- Duty status*
- Date and time of each change of duty status*
- Location of CMV when the CMV's engine is turned on and turned off, at each change of duty status, and at intervals of no more than 60 minutes when the CMV is in motion.*
- Starting time for each 24-hour period (*e.g.,* 12 midnight, 12 noon). This is a requirement for paper RODS and carries over to ELDs. The reason is that many elements of the HOS regulations are based on activities within 24-hour periods.*
- Hours in each duty status to 1-minute accuracy.*
- Special driving mode status (*e.g.,* personal conveyance, yard move).*
- Log of user activity (''user'' is generally the driver, but could be a technician test-driving the CMV or a yard-hotelier repositioning the CMV)*
- 17-digit vehicle identification number (VIN)*

RECORD SOURCE CATEGORIES:

CMV drivers and motor carrier submit records to assist authorized safety officials to determine if drivers comply with applicable HOS regulations.

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), all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

System Specific Routine Uses

1. To Motor Carrier Safety Assistance Program (MCSAP) State partner agencies for use during investigations, safety audits, and roadside inspections of motor carriers. This routine use enables the MCSAP agencies to review and analyze motor carrier and driver HOS practices and data to enforce the HOS regulations.

Department General Routine Uses

2. In the event that a system of records maintained by DOT to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto.

3a. Routine Use for Disclosure for Use in Litigation. It shall be a routine use of the records in this system of records to disclose them to the Department of Justice or other Federal agency conducting litigation when—(a) DOT, or any agency thereof, or (b) Any employee of DOT or any agency thereof, in their official capacity, or (c) Any employee of DOT or any agency thereof, in their individual capacity where the Department of Justice has agreed to represent the employee, or (d) The United States or any agency thereof, where DOT determines that litigation is likely to affect the United States, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or other Federal agency conducting the litigation is deemed by DOT to be relevant and necessary in the litigation, provided, however, that in each case, DOT determines that disclosure of the records in the litigation is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

3b. Routine Use for Agency Disclosure in Other Proceedings. It shall be a routine use of records in this system to disclose them in proceedings before any court or adjudicative or administrative body before which DOT or any agency thereof, appears, when—(a) DOT, or any agency thereof, or (b) Any employee of DOT or any agency thereof in their official capacity, or (c) Any employee of DOT or any agency thereof in their individual capacity where DOT has agreed to represent the employee, or (d) The United States or any agency thereof, where DOT determines that the proceeding is likely to affect the United States, is a party to the proceeding or has an interest in such proceeding, and DOT determines that use of such records is relevant and necessary in the proceeding, provided, however, that in each case, DOT determines that disclosure of the records in the proceeding is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

4. Disclosure may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual. In such cases, however, the Congressional office does not have greater rights to records than the individual. Thus, the disclosure may be withheld from delivery to the individual where the file contains investigative or actual information or other materials which are being used, or are expected to be used, to support prosecution or fines against the individual for violations of a statute, or of regulations of the Department based on statutory authority. No such limitations apply to records requested for Congressional oversight or legislative purposes; release is authorized under 49 CFR 10.35(9).

5. One or more records from a system of records may be disclosed routinely to the National Archives and Records Administration (NARA) in records

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

6. DOT may make available to another agency or instrumentality of any government jurisdiction, including State and local governments, listings of names from any system of records in DOT for use in law enforcement activities, either civil or criminal, or to expose fraudulent claims, regardless of the stated purpose for the collection of the information in the system of records. These enforcement activities are generally referred to as matching programs because two lists of names are checked for match using automated assistance. This routine use is advisory in nature and does not offer unrestricted access to systems of records for such law enforcement and related antifraud activities. Each request will be considered on the basis of its purpose, merits, cost effectiveness and alternatives using Instructions on reporting computer matching programs to the Office of Management and Budget, OMB, Congress, and the public, published by the Director, OMB, dated September 20, 1989.

7. DOT may disclose records from this system, as a routine use, to appropriate agencies, entities, and persons when (1) DOT suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DOT 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 DOT 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 DOT's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

8. DOT may disclose records from this system, as a routine use, to the Office of Government Information Services for the purpose of (a) resolving disputes between FOIA requesters and Federal agencies and (b) reviewing agencies' policies, procedures, and compliance in order to recommend policy changes to Congress and the President.

9. DOT may disclose records from the system, as a routine use, to contractors and their agents, experts, consultants, and others performing or working on a contract, service, cooperative agreement, or other assignment for DOT, when necessary to accomplish an agency function related to this system of records.

10. DOT may disclose records from this system, as a routine use, to an agency, organization, or individual for the purpose of performing audit or oversight operations related to this system of records, but only such records as are necessary and relevant to the audit or oversight activity. This routine use does not apply to intra-agency sharing authorized under section (b)(1) of the Privacy Act.

11. DOT may disclose from this system, as a routine use, records consisting of, or relating to, terrorism information (6 U.S.C. 485(a)(5)), homeland security information (6 U.S.C. 482(f)(1)), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, ''Information Sharing Environment'', November 22, 2006) to a Federal, State, local, Tribal, territorial, foreign government and/or multinational agency, either in response to its request or upon the initiative of the Component, for purposes of sharing such information as is necessary and relevant for the agencies to detect, prevent, disrupt, preempt, and mitigate the effects of terrorist activities against the territory, people, and interests of the United States of America, as contemplated by the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458) and Executive Order 13388 (October 25, 2005).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored electronically on a contractor-maintained cloud storage service.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

ELD and driver records may be retrieved by the following data elements: ELD file submittal date; Carrier Name, Carrier USDOT Number; Driver First Name; Driver Last Name; Driver License State; Driver License Number; ELD File Comment. ELD vendor records may be retrieved by the following data elements: ELD vendor name, phone number, address, email, ELD device name, ELD Identifier, ELD registration ID. Records of a driver may be retrieved by the following data elements: driver name, license state, license number, motor carrier name, USDOT number, investigation code, and file submittal date.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Motor carriers must retain records for six months from date of receipt. In accordance with FMCSA's MCMIS record schedule Job Number N1–557–05–007, item 5a for MCMIS inputs, where the data will be deleted after the information is converted or copied to the MCMIS master data files, backed up, and verified.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. Appropriate controls have been imposed to minimize the risk of compromising the information that is being stored and ensuring confidentiality of communications using tools such as encryption, authentication of sending parties, and compartmentalizing databases; and employing auditing software. ELD data is encrypted at rest and in transit. Access to records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. All personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

RECORD ACCESS PROCEDURES:

Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request to the System Manager in writing to the address provided under ''System Manager and Address.''

- When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the request must conform with the Privacy Act regulations set forth in 49 CFR part 10. The individual must verify their identity by providing their full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. No specific form is required. In addition, the individual should:
- Explain why the individual believes the Department would possess information on him/her;
- Identify which component(s) of the Department the individual believes may have the information about them;
- Specify when the individual believes the records would have been created; and

• Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If an individual seeks records pertaining to another living individual, the requesting individual must include a statement from the second individual certifying their agreement to the requested access. Without the above information, the Department may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

FMCSA depends upon drivers and motor carriers to submit data as accurately as possible. The ELD drivers review their records of duty status daily and certify their correctness prior to submission to the motor carriers and FMCSA. If a driver notices that information is missing or contains errors, the driver would use the motor carrier's ELD device to make the necessary corrections or enter missing information.

After a driver submits his or her certified daily records to the motor carrier, the motor carrier reviews those records. If the carrier identifies additional errors, the carrier may request the driver to make additional edits. However, motor carriers or dispatchers that suggest a change to a drivers' HOS records following submission to the carrier are to have the driver confirm or reject, and then re-certify the accuracy of the record. All edits have to be annotated to document the reason for the change. This procedure is intended to protect the integrity of the ELD records and to prevent related instances of potential driver harassment.

In support of a roadside inspection, investigation, or safety audit, a motor carrier submits his or her certified daily records to safety officials for an HOS review, the safety official may cite a violation based on these records.

FMCSA has a redress process to challenge inspection, investigation, and safety audit data. The process, called DataQs, is accessible at *https://dataqs.fmcsa.dot.gov.* DataQs provides an electronic method for motor carriers and drivers to file concerns about information maintained in FMCSA systems (principally, roadside inspection results included in MCMIS). The DataQs system automatically forwards data concerns to the appropriate Federal or State office for processing and resolution. Any challenges to data provided by State agencies are resolved by the appropriate State agency. The system also allows filers to monitor the status of each filing.

Under the DataQs process, FMCSA cannot ''correct the information associated with the ELD records'' that are stored in the motor carrier's information systems. If an interstate CMV driver is incorrectly identified in an enforcement action, the DataQs system provides an avenue for a driver or motor carrier to request FMCSA to correct enforcement information that it may store in its own information systems.

Individuals seeking to contest the content of any record pertaining to themselves in this system may also contact the System Manager following the Privacy Act procedures in 49 CFR part 10, subpart E, Correction of Records. Written requests for correction must conform with the Privacy Act regulations set forth in 49 CFR part 10. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the FMCSA Freedom of Information Act Officer *https://www.fmcsa.dot.gov/foia/foia-requestsor foia2@dot.gov.*

NOTIFICATION PROCEDURES:

Individuals seeking to contest the content of any record pertaining to themselves in the system may contact the System Manager following the procedures described in ''Record Access Procedures'' above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Issued in Washington, DC.

Karyn Gorman,

Departmental Chief Privacy Officer.

[FR Doc. 2024–10811 Filed 5–16–24; 8:45 am]

BILLING CODE 4910–9X–P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Publication of the List of Services, Software, and Hardware Incident to Communications

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Publication of a list of items determined to be incident to communications in the Iranian Transactions and Sanctions Regulations.

SUMMARY: The Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing a list of items that have been determined to be incident to communications and therefore authorized for export or reexport to Iran under a general license issued pursuant to the Iranian Transactions and Sanctions Regulations (ITSR). The list previously existed as an annex to ITSR General License D and its subsequent iterations, General License D–1 and General License D–2, all of which were previously made available on OFAC's website. Concurrent with publication of the list, OFAC is publishing an updated version of the list that, effective 30 days after publication, will restrict the computing power of certain items on the list.

DATES: This list is effective May 17, 2024.

FOR FURTHER INFORMATION CONTACT: OFAC: Assistant Director for Licensing, 202–622–2480; Assistant Director for Regulatory Affairs, 202–622–4855; or Assistant Director for Sanctions Compliance & Evaluation, 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The text of the List of Services, Software, and Hardware Incident to Communications is available on the Iran Sanctions page on OFAC's website, and additional information concerning OFAC is available on OFAC's website (*www.treasury.gov/ofac*).

Background

On May 30, 2013, OFAC, in consultation with the Departments of State and Commerce, issued General License (GL) D under the Regulations. GL D was made available on OFAC's website and in the **Federal Register** (78 FR 43278, July 19, 2013). GL D authorized the exportation or reexportation, directly or indirectly, from the United States or by U.S. persons, wherever located, to persons in Iran of additional services, software, and hardware incident to personal communications, including fee-based versions of the software and services authorized in § 560.540. GL D also contained an Annex that listed items authorized for export or reexport that had been determined to be incident to personal communications.

On February 7, 2014, OFAC issued GL D–1, which replaced and superseded GL D in its entirety. GL D–1 was made available on OFAC's website and in the **Federal Register** (79 FR 13736, March 11, 2014). GL D–1 clarified certain aspects of GL D and added certain new