Information collection	Respondents	Total annual responses	Hours per response	Total annual burden hours
Testing Requirements for Non-Bulk Packaging—Reporting	5,000	15,000	2.016	30,250
Additional Test Reports—Reporting	10	30	2	60
Test Reports—Recordkeeping	100	1,000	0.1	100
Closure Instructions—Reporting	500	500	2	1,000
Closure Instructions—Recordkeeping	16,080	16,080	0.083	1,340

Affected Public: Each non-bulk packaging manufacturer that tests packagings to ensure compliance with the HMR.

Annual Reporting and Recordkeeping Burden:

Total Number of Respondents: 21,690.

Total Annual Responses: 32,610.

Total Annual Burden Hours: 32,750.

Frequency of Collection: On occasion.

Title: Hazardous Materials Public Sector Training and Planning Grants.

OMB Control Number: 2137–0586.

Summary: This OMB control number describes the information collections in parts 110 of the HMR pertaining to the procedures for reimbursable grants for public sector planning and training in support of the emergency planning and training efforts of States, Indian tribes, and local communities to manage hazardous materials emergencies, particularly those involving transportation. Sections in this part address information collection and recordkeeping with regard to applying for grants, monitoring expenditures, and reporting and requesting modifications.

The following is a list of the information collections and burden estimates associated with this OMB Control Number:

Information collection	Respondents	Total annual responses	Hours per response	Total annual burden hours
Hazardous Materials Grants Applications	62	62	83.26	5,162

Affected Public: State and local governments, Indian Tribes.

Annual Reporting and Recordkeeping Burden:

Total Annual Respondents: 62.

Annual Responses: 62.

Annual Burden Hours: 5,162.

Frequency of Collection: On occasion.

Issued in Washington, DC, on August 23, 2023.

T. Glenn Foster,

Chief, Regulatory Review and Reinvention Branch, Office of Hazardous Materials Safety, Pipeline and Hazardous Materials Safety Administration.

[FR Doc. 2023–18617 Filed 8–28–23; 8:45 am]

BILLING CODE 4910–60–P

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

[Docket No. DOT–OST– 2023–0069]

Privacy Act of 1974; System of Records

AGENCY: Office of the Departmental Chief Information Officer, Office of the Secretary of Transportation, DOT.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the United States Department of Transportation proposes to rename, update and reissue a Department of Transportation (DOT) system of records notice titled, ''Department of Transportation, Federal Aviation Administration; DOT/FAA 854 Small Unmanned Aircraft Systems (sUAS) Waivers and Authorizations.'' The name of the SORN will be changed to ''Unmanned Aircraft System (UAS) Waivers and Authorizations''. The modification of the system of records notice (hereafter referred to as ''Notice'') allows the Federal Aviation Administration (FAA) to collect and maintain records on individuals operating small unmanned aircraft systems (hereinafter ''sUAS'') who request and receive authorizations to fly their sUAS in controlled airspace or waivers to fly their sUAS outside of the requirements of the Code of Federal Regulations (CFR) and to review and approve Certificate of Waiver or Authorizations (COA) applications.

DATES: Submit comments on or before September 28, 2023. The Department may publish an amended Systems of Records Notice (hereafter ''Notice'') in light of any comments received. This modified system will be effective immediately and the modified routine uses will be effective September 28, 2023.

ADDRESSES: You may submit comments, identified by docket number DOT–OST–2023–0069 by any of the following methods:

- *Federal e-Rulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments.
- *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.
- *Fax:* (202) 493–2251.

Instructions: You must include the agency name and docket number DOT–OST–2023–0069. All comments received will be posted without change to *https://www.regulations.gov,* including any personal information provided.

Privacy Act: Anyone is able to search the electronic form of all comments received in any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the Department of Transportation's complete Privacy Act statement in the **Federal Register** published on April 11, 2000 (65 FR 19477–78), or you may visit *http://DocketsInfo.dot.gov.*

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov* or to the street address listed above. Follow the online instructions for accessing the docket.

FOR FURTHER INFORMATION CONTACT: For questions, please contact: Karyn Gorman, Departmental Chief Privacy Officer, Privacy Office, Department of Transportation, Washington, DC 20590; *privacy@dot.gov;* or 202–366–3140.

SUPPLEMENTARY INFORMATION:

Notice Update

This Notice update includes substantive changes to the following sections: system name, system location, system manager, authority, purpose, routine uses, policies and practices for retrieval of records, and policies and practices for retention and disposal of records.

Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Transportation (DOT)/Federal Aviation Administration (FAA) proposes to rename, update and reissue a DOT system of records titled, ''DOT/FAA 854, Small Unmanned Aircraft Systems (sUAS) Waivers and Authorizations.'' This update results from the FAA Reauthorization Act of 2018, Public Law 115–254 section 44807, *Special Rules for Certain Unmanned Aircraft Systems,* which directs the FAA to integrate unmanned aircraft systems (UAS) safely into the National Airspace System (NAS). Individuals operating UAS civil aircraft under 14 CFR part 91, which meet the requirements established in 49 U.S.C. 44807, can request and receive a special airworthiness certificate, restricted category aircraft (21.25), Type Certificate, or a Section 44807 exemption with Certificate of Waiver or Authorization. The FAA issues a Certificate of Waiver or Authorization (COA) that permits persons, public agencies, organizations, and commercial entities to operate unmanned aircraft, for a particular purpose, in a particular area of the NAS as an exception to FAA Regulations. Consequently, this update expands the Notice's scope to cover individuals operating UAS under the provisions of 14 CFR part 91. The previous version of this Notice only applied to persons flying sUAS under the provisions of 14 CFR part 107 or flying sUAS in limited recreational operations pursuant to 49 U.S.C. 44809(a).

Under current law, persons flying sUAS under the provisions of 14 CFR part 107 or flying sUAS in limited recreational operations pursuant to 49 U.S.C. 44809(a) may not operate sUAS in Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport unless the person has received authorization to operate from the FAA. sUAS operators under 14 CFR part 107, who are also referred to as remote pilots in command, may request waivers of airspace and operational rules applicable to sUAS requirements under 14 CFR part 107.

The FAA uses two systems to process the waiver and airspace authorization requests subject to this notice. The first is a web-based system where sUAS operators who seek a waiver or an authorization may request one by electronically completing a form on the FAA website.[1] The FAA reviews the information the applicant provides and determines whether it can ensure safety in the national airspace when granting the waiver or authorization. Often, such grants will include provisions to which the requestor must adhere, to mitigate the risk associated with the waiver or authorization.

sUAS operators may also request authorization through third parties qualified to offer services by the FAA under the Low Altitude Authorization and Notification Capability (hereinafter ''LAANC''). These third parties, called UAS Service Suppliers (hereinafter ''USS''), enter into agreements with the FAA to automate and expedite the process by which sUAS operators receive authorization from the FAA to fly in the aforementioned airspace. The USS develop applications that enable sUAS operators to submit requests for authorization to the FAA where the requests are evaluated against predetermined criteria contained in LAANC. This enables sUAS operators to quickly and efficiently obtain authorizations to operate in Class B, C, D and within the lateral boundaries of surface area E designated for an airport. The number of USS available to the public, and the locations where LAANC is available, are updated on the FAA website located at *https://www.faa.gov/uas/programs_partnerships/data_exchange/.*

Additionally, under current law, persons flying UAS under the provisions of 14 CFR part 91 that cannot comply with all regulatory requirements may not operate UAS in the NAS unless the person has received authorization to operate from the FAA. UAS operators may request a COA under 14 CFR part 91 using web-based systems or they can use a PDF version of the Form 7711–2. The COA is issued by the FAA to a UAS operator for a specific unmanned aircraft (UA) activity.

The FAA uses a web-based application to process the COA. After the submission of a COA application, the FAA conducts a comprehensive operational and technical review. Additionally, the applicant can also apply for the COA using a PDF version of the Form 7711–2, Application for Certificate of Waiver or Authorization.[2] If necessary, provisions or limitations may be imposed as part of the approval to ensure the UAS can operate safely with other airspace users. In most cases, the FAA will provide a formal response within 60 business days from the time of submission.

Specifically, FAA is updating this Notice to make the following substantive changes:

1. The Notice title is being changed to Unmanned Aircraft System (UAS) Waivers and Authorizations, since the scope of the records has expanded to include individuals operating UAS under the provisions of 14 CFR part 91.

2. The system location is being updated to include and update the location of all systems covered by this Notice.

3. The system manager is being updated to include the system managers and contact information for all systems covered by this Notice.

4. The purpose is being updated to include an explanation that the system that will be used to facilitate review and approval of COA applications submitted under 14 CFR part 91 for all classes of airspace and ensure the operator is able to operate in a safe manner. The purpose is also being updated to clarify that the system will also be used to assist other government agencies in investigating or prosecuting violations or potential violations of law. UAS operators who operate their UAS in certain airspace without the proper authorization or waiver may be subject to a variety of civil, criminal, or regulatory penalties depending on the circumstances. Therefore, it is critical for law enforcement to understand whether a UAS flying in certain airspace has sought and received an authorization or waiver from the FAA if there is an indication of a violation of law.

5. The authority for maintenance of the system is being updated to remove § 333, Special Rules for Certain Unmanned Aircraft Systems, which has been repealed, and add its replacement, 49 U.S.C. 44807 *Special Rules for Certain Unmanned Aircraft Systems.* This section is also being updated to include 14 CFR part 91, ''General Operating and Flight Rules'', since the scope of this Notice is being expanded to include COA operations under these authorities.

6. The routine use section is being updated to add the following new system specific routine use: Disclosure of information to government agencies, whether Federal, State, Tribal, local or

[1] OMB Numbers 2120–0768, 2120–0776, and 2120–0796.

[2] OMB Number 2120–0027.

foreign, information necessary or relevant to an investigation of a violation or potential violation of law, whether civil, criminal, or regulatory, that the agency is charged with investigating or enforcing; as well as to government agencies responsible for threat detection in connection with critical infrastructure protection. This use is compatible with the purpose of this system as this system is intended to ensure that sUAS operators are operating their sUAS in accordance with the requirements of 14 CFR part 107 and 49 U.S.C. 44809 and to ensure that UAS operators are operating their UAS in accordance with the requirements of 14 CFR part 91. In addition, this routine use is compatible with the system's oversight purpose and its purpose for assisting other government agencies investigate or prosecute violations or potential violations of law.

7. The retrieval section is being updated to include that records can be retrieved by a unique generated number (including, but not limited to, application number and COA number).

8. The records retention and disposal section is being updated to include the retention schedule for airspace authorization records maintained by LAANC. The records were previously maintained indefinitely until the FAA's records schedule was approved by the National Archives and Records Administration (NARA). NARA has since approved the FAA's schedule, DAA–0237–2019–0011, and therefore LAANC records will be destroyed three years after authorization is revoked or canceled. This notice also adds NARA retention schedule DAA–0237–2023–0004 for COA Applications (COA Application Processing System [CAPS] and COA Application in DroneZone [CADZ]). The retention schedule is with NARA for approval and the FAA is proposing to retain the records for three years after authorization is revoked or canceled. FAA will maintain the records indefinitely until NARA has approved the schedule.

A. Description of Records

The FAA's regulations at 14 CFR part 107 governing operation of sUAS permits operators to apply for certificates of waiver to allow a sUAS operation to deviate from certain provisions of 14 CFR part 107, if the FAA Administrator finds the operator can safely conduct the proposed operation under the terms of a certificate of waiver. Operators flying under 14 CFR part 107 or flying limited recreational operations under 49 U.S.C. 44809(a) may request authorization to enter controlled airspace (Class B, Class C, or Class D airspace, or within the lateral boundaries of the surface area of Class E airspace designated for an airport). The FAA assesses requests for waivers on a case-specific basis that considers the proposed sUAS operation, the unique operating environment, and the safety mitigations provided by that operating environment. Accordingly, this Notice covers documents relevant to both waivers of certain provisions of 14 CFR part 107 as well as authorizations to fly in controlled airspace.

Additionally, the FAA's regulations governing operations under 14 CFR part 91 permit operators to apply for a COA to allow a UAS operation to deviate from certain provisions of 14 CFR part 91 if the FAA Administrator finds the operator can safely conduct the proposed operation under the terms of a COA. Operators flying under 14 CFR part 91 may request authorization to operate in the NAS. The FAA assesses requests for waivers on a case-specific basis that considers the proposed UAS operation, the unique operating environment, and the safety mitigations provided by that operating environment. Accordingly, this Notice covers documents relevant to both waivers and authorizations of certain provisions of 14 CFR part 91.

At times, operators requesting waivers and authorizations under the regulations described above are companies or other non-person entities, rather than individuals. Because the Privacy Act applies only to individuals, this Notice applies only to waiver and authorization records where the owner or operator requesting the waiver is an individual, and does not apply to records pertaining to non-person entities.

1. Waivers

To obtain a certificate of waiver, an applicant must submit a request containing a complete description of the proposed operation and a justification, including supporting data and documentation as necessary, to establish the proposed operation can be conducted safely under the terms of the requested certificate of waiver. The FAA expects that the time and effort the operator will put into the analysis and data collection for the waiver application will be proportional to the specific relief requested. The FAA will analyze all requests for a certificate of waiver and will provide responses as timely as possible with more complex waivers requiring more time than less complex ones. If a certificate of waiver is granted, that certificate may include additional conditions and limitations designed to ensure that the sUAS operation can be conducted safely. While all decisions are made against the same criteria, decisions are made on a situation specific basis.

For airspace authorization requests to operate a sUAS in Class B, information collected relevant to waivers includes: name of person requesting the waiver; contact information for person applying for the waiver (telephone number, mailing address, and email address); remote pilot in command name; remote pilot in command airmen certification number and rating; remote pilot in command' contact information; aircraft registration number; aircraft manufacturer name and model; submission reference code; regulations subject to waiver; requested date and time operations will commence and conclude under the waiver; flight path information, including but not limited to altitude and coordinates; safety justification; and description of proposed operations.

2. Airspace Authorizations

For Class C, Class D or within the lateral boundaries of the surface area of Class E airspace designated for an airport, a remote pilot in command may seek either automatic approval or a request for further coordination from the FAA. Automatic approvals are completed by checking against pre-determined FAA-approved altitude values and locations within the aforementioned airspace. Requests sent through the FAA website are manually checked against the pre-determined values to either approve or deny the request. As this method requires manual approval and is not scalable to the increasing numbers of requests for authorization, the time for the sUAS operator to receive a response is variable.

Requests sent through the LAANC are approved or denied via an automated process and operators receive near real time notice of either an approval or denial of the authorization request. ''Requests for further coordination'' are needed for those authorization requests for operations that are within the aforementioned airspace, under 400 feet of altitude, and for a location and altitude that has not been pre-determined by the FAA to be safe without further consideration. These requests for further coordination are sent via either the FAA website or through LAANC for 14 CFR part 107 operations and routed for approval or denial to the local Air Traffic Control (ATC) facility where the requested operation would take place, to make an

approval decision. The ATC facility has the authority to approve or deny aircraft operations based on traffic density, controller workload, communications issues, or any other types of operational issues that could potentially impact the safe and efficient flow of air traffic in that airspace. If necessary to approve a sUAS operation, ATC may require mitigations such as altitude constraints and direct communication. ATC may deny requests that pose an unacceptable risk to the NAS and cannot be mitigated.

Information collected relevant to airspace authorizations requested using the non-automated method includes: aircraft operator name; aircraft owner name; name of person requesting the authorization; contact information for the person applying for the authorization; remote pilot in command name; remote pilot in command contact information; remote pilot in command certificate number; aircraft manufacturer name and model; aircraft registration number; requested date and time operations will commence and conclude; requested altitude applicable to the authorization; and description of proposed operations.

Information collected relevant to airspace authorizations requested using the automated method LAANC includes: name of pilot in command; contact telephone number of remote pilot in command; start date, time, and duration of operation; maximum altitude; geometry; airspace class(es); submission reference code; safety justification for requests for further coordination non-auto-authorized operation; and aircraft registration number.

3. Certificate of Waiver or Authorization Associated With Part 91 Civil UAS Operation

To obtain a certificate of waiver or authorization an applicant completes the FAA Form 7711–2. An applicant can submit a PDF form 7711–2 to *9-AJV-115-UASOrganization@faa.gov* or apply online. The legacy system Certificate of Authorization Application Processing System (CAPS) is currently used for processing of these applications; however, this will eventually be replaced by the Certificate of Authorization (COA) Application in the DroneZone (CADZ) system, which is currently in development. The Application for Certificate of Waiver or Authorization collects the name, address, email address and phone number from the applicant, along with details of the operation needed to evaluate the application. Once the applicant submits the application, the application system (CAPS/CADZ) will automatically generate a unique numerical draft number used to track the application. The applicant must acknowledge several statements called declarations. The declarations section requires Yes or No responses from the applicant that certify or declare their type of operation and associated authorization. CAPS/CADZ also collects information about the requested operation, flight operations area/plan, UAS specifications, and any flight crew qualifications. The application is submitted to a Processor for their review and to ensure the appropriate information is provided to evaluate the application including any attachments that may be needed.

Once the application is submitted, a COA Processor will work with the applicant to clarify or correct inconsistencies in the application. The COA Processor will have the ability to return the application to the applicant for further refinement or submit it to the next reviewer (Air Traffic Control Specialists or Aviation Safety Inspector). This review process is repeated until all necessary parties have approved the application or it is determined that it cannot be approved. Once the COA is granted and the COA becomes active, a signed PDF copy of the COA is sent to the applicant. If disapproved, the COA processor sends a disapproval letter stating the reason for the disapproval.

Privacy Act

The Privacy Act (5 U.S.C. 552a) governs the means by which the Federal Government collects, maintains, and uses personally identifiable information (PII) in a System of Records. A ''System of Records'' is a group of any records under the control of a Federal agency from which information about individuals is retrieved by name or other personal identifier. The Privacy Act requires each agency to publish in the **Federal Register** a System of Records Notice (SORN) identifying and describing each System of Records the agency maintains, including the purposes for which the agency uses PII in the system, the routine uses for which the agency discloses such information outside the agency, and how individuals to whom a Privacy Act record pertains can exercise their rights under the Privacy Act (*e.g.,* to determine if the system contains information about them and to contest inaccurate information). In accordance with 5 U.S.C. 552a(r), DOT has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

Department of Transportation, Federal Aviation Administration, DOT/FAA—854 Unmanned Aircraft Systems (UAS) Waivers and Authorizations.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

1. COA Application Processing System (CAPS): [3] Enterprise Data Center (EDC) located within the AIT Network at the Mike Monroney Aeronautical Center (MMAC), Oklahoma City, OK.

2. Low Altitude Authorization and Notification Capability (LAANC) and Part 107 Authorization and Waivers: Amazon Web Services (AWS) US-West and Oregon Region of the AWS East/West Public Cloud.

SYSTEM MANAGER(S) AND ADDRESS:

1. COA Application Processing System (CAPS): [4] Manager, UAS Policy Team (AJV–P22), Air Traffic Organization, Federal Aviation Administration, 600 Independence Avenue SW—Suite #5E21TS Washington, DC 20591 (Wilbur Wright Federal Building—FOB 10B). Contact information is mailbox: *9-AJV-115-UASOrganization@faa.gov.*

2. Low Altitude Authorization and Notification Capability and Part 107 Authorization and Waivers: Manager, Amazon Web Services US East/West Public Cloud. Contact information for system manager is *UAShelp@faa.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 106(g), Duties and powers of Administrator; 49 U.S.C. 40101, Policy; 49 U.S.C. 40103, Sovereignty and use of airspace; 49 U.S.C. 40106, Emergency powers; 49 U.S.C. 40113, Administrative; 49 U.S.C. 44701, General requirements; FAA Modernization and Reform Act of 2012, Public Law 112–95 (''FMRA''); 14 CFR part 91, ''General Operating and Flight Rules''; 14 CFR part 107, subpart D, ''Waivers''; 14 CFR 107.41, ''Operation in certain airspace''; and 49 U.S.C. 44807 and 44809(a).

PURPOSE(S):

The purpose of this system is to receive, evaluate, and respond to requests for authorization to operate a sUAS in Class B, C or D airspace or within the lateral boundaries of the surface area of Class E airspace

[3] CAPS will be replaced by CADZ and the system will be located at Amazon Web Services (AWS) US-West and Oregon Region of the AWS East/West Public Cloud.

[4] CAPS will be replaced by CADZ and the system manager will be the same as LAANC and Part 107 Waivers.

designated for an airport, and evaluate requests for a certificate of waiver to deviate safely from one or more sUAS operational requirements specified in 14 CFR part 107. The system will also be used to facilitate FAA's review and approval of COA applications submitted under 14 CFR part 91 for all classes of airspace and ensure the operator is able to operate in a safe manner. The FAA also will use this system to support FAA safety programs and agency management, including safety studies and assessments. The FAA may use contact information provided with requests for waivers or authorizations to provide owners and operators' information about potential unsafe conditions and educate owners and operators regarding safety requirements for operation. The FAA will also use this system to maintain oversight of FAA issued waivers and authorizations, and records from this system may be used by FAA for enforcement purposes. The FAA will use this system to assist other government agencies with investigating or prosecuting violations or potential violations of law.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Aircraft operators, aircraft owners, and persons requesting a waiver or authorization.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name; contact information to include: mailing address, telephone number, and email address; responses to inquiries concerning the applicant's previous and current waivers; certificate number; aircraft manufacturer name and model; aircraft registration number; unique generated number (including, but not limited to, application number and COA number); regulations subject to waiver or authorization; requested date and time operations will commence and conclude under waiver or authorization; flight path information, including but not limited to the requested altitude and coordinates of the applicable waiver or authorization; description of proposed operations; specifications; geometry (center point with radius or Geo/JSON polygon); airspace class(es); submission reference code; safety justification for non-auto-authorized operations.

RECORD SOURCE CATEGORIES:

Records are obtained from aircraft operators, aircraft owners, persons requesting a waiver or authorization, manufacturers of aircraft, maintenance inspectors, mechanics, and FAA officials. Records are also obtained on behalf of individuals through USS.

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

In addition to other 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 outside DOT as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

System Specific Routine Uses:

1. To the public, waiver applications and decisions, including any history of previous, pending, existing, or denied requests for waivers applicable to the sUAS at issue for purposes of the waiver, and special provisions applicable to the sUAS operation that is the subject of the request. Email addresses and telephone numbers will not be disclosed pursuant to this Routine Use. Airspace authorizations the FAA issues also will not be disclosed pursuant to this Routine Use, except to the extent that an airspace authorization is listed or summarized in the terms of a waiver.

2. To law enforcement, when necessary and relevant to a FAA enforcement activity.

3. To the National Transportation Safety Board (NTSB) in connection with its investigation responsibilities.

4. To government agencies, whether Federal, State, Tribal, local or foreign, information necessary or relevant to an investigation of a violation or potential violation of law, whether civil, criminal, or regulatory, that the agency is charged with investigating or enforcing; as well as, to government agencies responsible for threat detection in connection with critical infrastructure protection.

Departmental Routine Uses:

5. 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.

6. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DOT decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

7. A record from this system of records may be disclosed, as a routine use, to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

8a. 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 (including a member of the Coast Guard), in his/her official capacity, or (c) Any employee of DOT or any agency thereof (including a member of the Coast Guard), in his/her 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.

8b. 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 his/her official capacity, or (c) Any employee of DOT or any agency thereof in his/her 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.

9. The information contained in this system of records will be disclosed to the Office of Management and Budget, OMB in connection with the review of private relief legislation as set forth in OMB Circular No. A–19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

10. 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 alleged 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).

11. One or more records from a system of records may be disclosed routinely to the National Archives and Records Administration in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

12. Routine Use for disclosure to the Coast Guard and to Transportation Security Administration. A record from this system of records may be disclosed as a routine use to the Coast Guard and to the Transportation Security Administration if information from this system was shared with either agency when that agency was a component of the Department of Transportation before its transfer to the Department of Homeland Security and such disclosure is necessary to accomplish a DOT, TSA or Coast Guard function related to this system of records.

13. 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.

14. It shall be a routine use of the information in any DOT system of records to provide to the Attorney General of the United States, or his/her designee, information indicating that a person meets any of the disqualifications for receipt, possession, shipment, or transport of a firearm under the Brady Handgun Violence Prevention Act. In case of a dispute concerning the validity of the information provided by DOT to the Attorney General, or his/her designee, it shall be a routine use of the information in any DOT system of records to make any disclosures of such information to the National Background Information Check System, established by the Brady Handgun Violence Prevention Act, as may be necessary to resolve such dispute.

15a. To appropriate agencies, entities, and persons when (1) DOT suspects or has confirmed that there has been a breach of the system of records; (2) DOT has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOT (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 DOT's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

15b. To another Federal agency or Federal entity, when DOT 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.

15. 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.

16. DOT may disclose records from this 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.

17. 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.

18. 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:

Individual records relevant to both waivers and airspace authorizations are maintained in electronic database systems.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records of applications for waivers and authorizations in the electronic database systems may be retrieved by UAS registration number, unique

generated number (including, but not limited to, application number and COA number), the manufacturer's name and model, the name of the current registered owner and/or organization, the name of the applicant and/or organization that submitted the request for waiver or authorization, the special provisions (if any) to which the FAA and the applicant agreed for purposes of the waiver or authorization, and the location and altitude, class of airspace and area of operations that is the subject of the request.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The FAA will retain LAANC waivers and airspace authorization records in this system of records in accordance with DAA–0237–2019–0011 (which covers anyone who wishes to fly a sUAS under the provisions of § 44809 or part 107). The FAA will destroy the records three years after authorization is revoked or canceled. Records Schedule 0237–2023–0004 for records maintained in CAPS and CADZ is currently pending NARA approval. The FAA is proposing to retain these records for three years after authorization is revoked or canceled. FAA will maintain the records indefinitely until NARA has approved the applicable schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system for waivers and airspace authorizations are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

Individuals seeking notification of whether this system of records contains information about them may contact the System Manager at the address provided in the section ''System manager.'' When seeking records about yourself from this system of records or any other Departmental system of records your request 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. If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

CONTESTING RECORDS PROCEDURE:

See ''Record Access Procedures'' above.

NOTIFICATION PROCEDURE:

See ''Records Access Procedures'' above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

A full notice of this system of records, DOT/FAA854 Requests for Waivers and Authorizations was published in the **Federal Register** on August 2, 2016 (81 FR 5078) and July 8, 2019 (84 FR 52512).

Issued in Washington, DC.

Karyn Gorman,

Departmental Chief Privacy Officer.

[FR Doc. 2023–18289 Filed 8–28–23; 8:45 am]

BILLING CODE 4910–9X–P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Action

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the name of one individual that has been placed on OFAC's Specially Designated Nationals and Blocked Persons List based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of this individual are blocked, and U.S. persons are generally prohibited from engaging in transactions with the individual.

DATES: See **SUPPLEMENTARY INFORMATION** section for applicable date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Andrea Gacki, Director, tel.: 202–622–2490; Associate Director for Global Targeting, tel.: 202–622–2420; Assistant Director for Licensing, tel.: 202–622–2480; Assistant Director for Regulatory Affairs, tel.: 202–622–4855; or the Assistant Director for Compliance, tel.: 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The Specially Designated Nationals and Blocked Persons List and additional information concerning OFAC sanctions programs are available on OFAC's website (*https://ofac.treasury.gov/*).

Notice of OFAC Action

On August 23, 2023, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following individual are blocked under the relevant sanctions authorities listed below.

Individual

1. SEMENOV, Roman (a.k.a. ''POMA''; a.k.a. ''ROMA''), Dubai, United Arab Emirates; DOB 08 Nov 1987; nationality Russia; Email Address *semenov.roma@gmail.com;* alt. Email Address *semenovroma@gmail.com;* alt. Email Address *semenov.roman@mail.ru;* alt. Email Address *poma@tornado.cash*; Gender Male; Digital Currency Address—ETH 0xdcbEfFBECcE100cCE9E4b153C4e15cB885643193; alt. Digital CurrencyA Address—ETH 0x5f48c2a71b2cc96e3f0ccae4e39318ff0dc375b2;a alt. Digital Currency Address—ETH 0x5a7a51bfb49f190e5a6060a5bc6052ac14a3b59f; alt. Digital Currency Address—ETH 0xed6e0a7e4ac94d976eebfb82ccf777a3c6bad921; alt. Digital Currency Address—ETH 0x797d7ae72ebddcdea2a346c1834e04d1f8df102b; alt. Digital Currency Address—ETH 0x931546D9e66836AbF687d2bc64B30407bAc8C568; alt. Digital Currency Address—ETH 0x43fa21d92141BA9db43052492E0DeEE5aa5f0A93; alt. Digital Currency Address—ETH 0x6be0ae71e6c41f2f9d0d1a3b8d0f75e6f6a0b46e; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210; Transactions Prohibited For Persons Owned or Controlled By U.S. Financial Institutions: North Korea Sanctions Regulations section 510.214; Passport 731969851 (Russia) (individual) [DPRK3] [CYBER2].

Designated pursuant to section l(a)(iii)(B) of Executive Order 13694 of April 1, 2015, ''Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'' 80 FR 18077, 3 CFR, 2015 Comp., p. 297, as amended by Executive Order 13757 of December 28, 2016, ''Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,'' 82 FR 1, 3 CFR, 2016 Comp., p. 659 (E.O. 13694, as amended) for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended.

Also designated pursuant to section 2(a)(vii) of Executive Order 13722 of March 15, 2016, ''Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea,'' 81 FR 14943, 3 CFR, 2016 Comp., p. 446