

The PRG was established pursuant to the requirements of the National Historic Preservation Act (NHPA) and its implementing regulations to plan for the decommissioning and disposition of the Nuclear Ship Savannah (NSS). PRG membership is comprised of officials from the U.S. Department of Transportation, MARAD, the U.S. Nuclear Regulatory Commission (NRC), the Advisory Council on Historic Preservation (ACHP), and the Maryland State Historic Preservation Officer (SHPO) and other consulting parties.

FOR FURTHER INFORMATION CONTACT:

Erhard W. Koehler, (202) 680–2066 or via email at marad.history@dot.gov. You may send mail to N.S. Savannah/ Savannah Technical Staff, Pier 13 Canton Marine Terminal, 4601 Newgate Avenue, Baltimore, MD 21224, ATTN: Erhard Koehler.

SUPPLEMENTARY INFORMATION:

I. Background

The decommissioning and disposition of the NSS is an Undertaking under Section 106 of the NHPA. Section 106 requires that federal agencies consider views of the public regarding their Undertakings; therefore, in 2020, MARAD established a Federal docket at <https://www.regulations.gov/docket/MARAD-2020-0133> to provide public notice about the NSS Undertaking. The federal docket was also used in 2021 to solicit public comments on the future uses of the NSS. MARAD is continuing to use this same docket to take in public comment, share information, and post agency actions.

The NHPA Programmatic Agreement (PA) for the Decommissioning and Disposition of the NSS is available on the MARAD docket located at www.regulations.gov under docket id “MARAD-2020-0133.” The PA stipulates a deliberative process by which MARAD will consider the disposition of the NSS. This process requires MARAD to make an affirmative, good-faith effort to preserve the NSS. The PA also establishes the PRG in Stipulation II. The PRG is the mechanism for continuing consultation during the effective period of the PA and its members consist of the signatories and concurring parties to the PA, as well as other consulting parties. The PRG members will provide individual input and guidance to MARAD regarding the implementation of stipulations in the PA.

PRG members and members of the public are invited to provide input by attending bi-monthly meetings and reviewing and commenting on

deliverables developed as part of the PA.

(Authority: 49 CFR 1.81 and 1.93; 36 CFR part 800; 5 U.S.C. 552b.)

By Order of the Maritime Administrator.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2024–13899 Filed 6–24–24; 8:45 am]

BILLING CODE 4910–81–P

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

[Docket No. DOT–OST–2024–0015]

Privacy Act of 1974; System of Records

AGENCY: Office of the Departmental Chief Information Officer, Office of the Secretary of Transportation, Department 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 (DOT), Office of the Secretary (OST), proposes to modify and reissue an existing system of records notice titled “Department of Transportation, Office of the Secretary; DOT/OST 035 Personnel Security Record System.” The system collects information on DOT employees, contractors, and members of the public to track and manage the information and records necessary to conduct employee suitability background investigations and determine eligibility for clearances. It is also used to maintain documentation for DOT employees who attend classified briefings outside of DOT, and non-DOT individuals attending meetings at DOT.

DATES: Submit comments on or before July 25, 2024. 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 July 25, 2024.

ADDRESSES: You may submit comments, identified by docket number DOT–OST–2024–0015 by one of the following methods:

- *Federal e-Rulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments.
- *Mail:* Department of Transportation Docket Management, Room W12–140, 1200 New Jersey Ave. SE, Washington, DC 20590.
- *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–2024–0015. 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.).

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

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:

Notice Updates

This Notice includes both substantive changes and non-substantive changes to the previously published Notice. Substantive changes have been made to the system location, system manager, authority for maintenance of the system, purposes, categories of individuals, categories of records, the record source categories, the routine uses of records maintained in the system, 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.

Non-substantive changes have been made to record access procedures, contesting record procedures, notification procedures, as well as revisions to align with the requirements of Office of Management and Budget Memoranda (OMB) A–108 and to ensure consistency with other Notices issued by the Department of Transportation.

Background

In accordance with the Privacy Act of 1974, the Department of Transportation proposes to update and reissue an existing system of records titled “DOT/OST 35 Personnel Security Record System.” This Notice covers information required for conducting and managing investigations for all federal and contract employees to obtain a badge, credential, or a national security

clearance as mandated by Executive Order 12968, as amended, "Access to Classified Information". Records in this system are collected, maintained, and used to track and manage the information and records necessary to conduct employee suitability background investigations and determine eligibility for clearances. In addition, records in this system are also used to maintain documentation for DOT employees who attend classified briefings outside of DOT, and non-DOT individuals attending classified meetings at DOT. The following substantive changes have been made to the Notice:

1. *System Location*: This Notice updates the system location to reflect the current location where individual records are submitted and processed to determine eligibility for clearances, conduct suitability background investigations and maintain documentation for DOT and non-DOT employees who attend classified briefings at DOT and outside of DOT. The previously published SORN identified a location that is no longer valid. All records covered in this Notice are maintained at the Department of Transportation, Office of the Secretary, 1200 New Jersey Ave SE, Suite W12-180, Washington DC 20590.

2. *System Manager*: This Notice updates the system manager to reflect to reflect current system Manager and inform the public the previous System Manager address is no longer valid. The new address is Principal, Office of Security, M-40, 1200 New Jersey Ave SE, Suite W12-180, Washington DC 20590.

3. *Authority*: This Notice updates the authorities to include additional authorities that cover the system of records and align with the requirements. The additional authorities include E.O. 12829; E.O. 12968, E.O. 13467; E.O. 13764; E.O. 9397, as amended by E.O. 13478; Security Executive Agent Directive 3; Security Executive Agent Directive 6; Security Executive Agent Directive 7; Homeland Security Presidential Directive 12; and National Industrial Security Program Operating Manual DoD 5220.22-M. These authorities establish the requirements for federal agencies to conduct initial and ongoing background suitability investigations of individuals seeking employment with or access to federal facilities and information systems. Investigations have been conducted under these authorities and they are consistent with the purposes of the published SORN.

4. *Purpose*: This Notice updates the purpose to better clarify purpose of the

system, identify additional data captured in the system, how the data is used, and maintained.

5. *Categories of Individuals*: This Notice updates the categories of individuals to reflect that information is collected from the members of the public, citizens and legal permanent residents, visitors to DOT for official business, detailees to DOT, current and former federal employees, and members of DOT contract workforce.

6. *Categories of Records*: This Notice updates categories of records collected in the system. The categories of records have been updated to include specifically individuals' names, date of birth, Social Security Numbers (SSNs), home address, and additional records that may assist in conducting employee suitability background investigations to determine eligibility for clearances.

7. *Records Source*: This Notice updates records source category and includes additional information collected directly from individuals and from other sources that are maintained in this system of records.

8. *Routine Uses*: This Notice updates routine uses to include the Department of Transportation's specific and general routine uses that specifically apply to this system and align with the purpose of the collection and maintenance of the data in the system. Also included are the routine uses that require agencies to share information in the event of an incident or breach in accordance with the OMB Memorandum M-17-12. OMB 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.

9. *Records Storage*: This Notice updates the policies and practices for storage of records to reflect that records previously completed on forms and typed pages and placed in a manual filing system and manual system control cards are now stored on paper and electronic storage media and maintained in a secure access control location.

10. *Records Retrieval*: This Notice updates and expands on how records are retrieved in the system. The previous SORN identified one method of retrieval of records. This Notice updates and expands the policies and practices for the retrieval of records to include retrievability by date of birth, Social Security Number (SSN), home address, and additional data elements that will assist in the background clearance of individuals.

11. *Retention and Disposal*: This Notice updates the retention and disposal policy to include the specific National Archives and Records

Administration (NARA) records retention and disposition schedule for all the records maintained in the system.

12. *Administrative, Technical, and Physical Safeguards*: This Notice is updated and expanded to ensure the public records in this system are protected in accordance with DOT and the National Institutes of Standards and Technology (NIST) applicable rules, policies and federal regulations.

The following non-substantive changes have been made to the Notice:

13. *Records Access*: This Notice updates the record access procedures to reflect the requirement for signed requests for records to be notarized or accompanied by a statement made under penalty of perjury in compliance with 28 U.S.C. 1746. The address to request access has also been updated to make certain the public's requests are sent to the appropriate address.

14. *Contesting Records and Notification Procedures*: This Notice is updated to direct individuals requesting a copy of their records who they should contact.

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 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:

DOT/OST 035—Personnel Security Enterprise System.

SECURITY CLASSIFICATION:

Unclassified, sensitive.

SYSTEM LOCATION:

Department of Transportation, Office of Security, 1200 New Jersey Ave SE, Suite W12-180, Washington, DC 20590.

SYSTEM MANAGER(S):

Principal, Office of Security, M-40 1200 New Jersey Ave SE, Suite W12-180, Washington DC 20590

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 322; E.O. 12829; E.O. 12968, E.O. 13467; E.O. 13764; E.O. 9397, (SSN) as amended by E.O. 13478; Security Executive Agent Directive 3; Security Executive Agent Directive 6; Security Executive Agent Directive 7; Homeland Security Presidential Directive 12; and DoD 5220.22-M, National Industrial Security Program Operating Manual.

PURPOSE(S) OF THE SYSTEM:

The system is used to track and manage the information and records necessary to conduct employee suitability background investigations and determine eligibility for clearances. The system captures data related to all aspects of pre-appointments, suitability and fitness determinations, security clearance processing, briefings, foreign travel, foreign contacts, procurement processes for classified contracts. It is also used to maintain documentation for DOT employees who attend classified briefings outside of DOT, and non-DOT individuals attending classified meetings at DOT. Additionally, the system allows the Department to collect metrics and report on operational performance.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Members of the public, citizens and legal permanent residents, visitors to DOT for official business, current and former federal employees, detailees to DOT from other federal agencies, and members of the DOT contract workforce.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name, date of birth, Social Security Number (SSN), home address, home phone number, personal data on investigative and employment provided by the individual. Reports of investigations, records of security and suitability determinations, records of access authorizations granted, documentation of security briefings/debriefings received, individual notifications of foreign travel for business or personal, records of security violations are also included.

Records of personnel security processing, personal data on investigative and employment forms completed by the individual.

Documented events of any classified national security violations.

RECORD SOURCE CATEGORIES:

Information provided by the subject of the DOT form, electronic background investigative request form and other related documents. Investigative sources contacted in personnel security investigations, baseline investigation for the issuance of Personal Identification Verification card (PIV card) and similar investigations for public trust and national security clearance eligibility; digital investigative reports reviewed at other Government agencies; personal history statements, employment applications and other data provided by the individual and/or other agencies.

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

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

System Specific Routine Use:

1. To the Department of Defense and other federal government agencies responsible for conducting background investigations, continuous evaluation, and continuous vetting in order to provide DOT with information relevant to their inquiries and investigations to evaluate, or make a determination regarding qualifications, suitability, or fitness for government employment to physically access federally-controlled facilities or information systems; eligibility for access to classified information or to hold a sensitive position; qualification or fitness to perform work for or on behalf of the government under contract, grant, or other agreement; or access to restricted areas.

Departmental 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.

3. 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.

4. 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.

5a. 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 his/her official capacity, or (c) Any employee of DOT or any agency thereof, 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.

5b. 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.

6. 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.

7. 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(a)(9).

8. 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.

9. 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.

10. 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.

11. DOT may disclose records from this system, as a routine use to appropriate agencies, entities and persons when (a) DOT suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) 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 (c) 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.

12. 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 Freedom of Information Act requesters and Federal agencies and (b) reviewing agencies' policies, procedures, and compliance in order to recommend policy changes to Congress and the President.

13. 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.

14. DOT may disclose records 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, 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.

16. 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 are maintained in paper and electronic storage media in accordance with the safeguards below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by name, date of birth, SSN, home address, home phone number, or other personal data elements on individuals who are subject of the investigation.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in the system are maintained in accordance with the following NARA records retention and schedules:

GRS 5.6—Item 120: Personal identification credentials and cards—Application and activation record: Destroy 6 years after the end of an employee or contractor's tenure (DAA-GRS-2021-0001-0005).

GRS 5.6—Item 130: Temporary and local facility identification and card access records: Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner (DAA-GRS-2021-0001-0006).

GRS 5.6—Item 170: Personnel suitability and eligibility investigative reports: Temporary. Destroy in accordance with the investigating agency instruction (DAA-GRS-2017-0006-0022).

GRS 5.6—Item 180: Personnel security and access clearance records. Records of people not issued clearances. Includes case files of applicants not hired: Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use (DAA-GRS-2017-0006-0024).

GRS 5.6—Item 181: Records of people issued clearances: Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use (DAA-GRS-2017-0006-0025).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Administrative safeguards: Access to data is role based and limited to those that have a need to know for the performance of their official duty. Personnel and contract support are required to attend and complete security and privacy awareness training. Controls are implemented to minimize the risk of information being compromised. Data in the system is protected in accordance with applicable rules and policies including all applicable Department automated systems security and access policies. All users must sign a non-disclosure agreement before granted role in system. Technical safeguards: An auditing function tracks all user activities in relation to data including access and modification. Controls include firewalls, intrusion detection, only role-based access and "need-to-know" specific to performance of their duties, can access control lists and other security methods. Physical Safeguards: Records are stored in an access-controlled office. Access is limited to authorized staff and visitors are only allowed escorted access if there

is a specific need for them to be in the space.

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." Information compiled solely for the purpose of determining suitability, contractor fitness, eligibility, or qualification for Federal civilian employment or access to classified information may be exempted from the access provisions pursuant to 5 U.S.C. 552a(k)(5).

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. Department policy requires the inquiry to include the name of the individual, mailing address, phone number or email address, a description of the records sought, and if possible, the location of the records. 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 RECORD PROCEDURES:

See "Records Access Procedures" above.

NOTIFICATION PROCEDURES:

See "Records Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Information compiled solely for the purpose of determining suitability, eligibility, or qualification for federal civilian employment or access to classified information may be exempted from the access provisions pursuant to 5 U.S.C. 552a(k)(1) and/or (5). See 80 FR 32039.

HISTORY:

A full notice of this system of records, DOT/OST 035—DOT OST 035—Personnel Security Enterprise System, was published in the *Federal Register* on April 11, 2000 (65 FR 19553).

Issued in Washington, DC.

Karyn Gorman,

Departmental Chief Privacy Officer.

[FR Doc. 2024-13825 Filed 6-24-24; 8:45 am]

BILLING CODE 4910-9X-P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Actions

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 names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN 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 these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

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

FOR FURTHER INFORMATION CONTACT:

OFAC: Bradley T. Smith, 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 Sanctions Compliance & Evaluation, tel.: 202-622-2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website (<https://www.treasury.gov/ofac>).

Notice of OFAC Actions

On June 20, 2024, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following persons are blocked under the relevant sanctions authority listed below.

Individuals

1. ARZATE GOMEZ, Kevin, Mexico; DOB 23 Jun 1992; POB Guerrero, Mexico; nationality Mexico; Gender Male; C.U.R.P. AAGK920623MGRMV09 (Mexico) (individual) [ILLICIT-DRUGS-EO14059]. Designated pursuant to section 1(a)(i) of Executive Order 14059 of December 15, 2021, "Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade," 86 FR 71549 (December 17, 2021) (E.O. 14059) for having engaged in, or attempted to engage in, activities or transactions that have materially contributed to, or pose a significant risk of materially contributing to, the international proliferation of illicit drugs or their means of production.

2. CAMACHO GOICOCHEA, Euclides (a.k.a. "Quilles"), Mexico; DOB 08 Aug 1972;