• *Fax:* (703) 705–6190, ATTN: Sandy Benevides.

• *Mail:* Helen Jackson, Designated Federal Officer, Stakeholder Engagement and Critical Infrastructure Resilience Division, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane, Mail Stop 0612, Arlington, VA 20598–0612.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number DHS–2018–0019. Comments received will be posted without alteration at *www.regulations.gov,* including any personal information provided.

Docket: For access to the docket and comments received by the NSTAC, please go to *www.regulations.gov* and enter docket number DHS–2018–0019.

A public comment period will be held during the meeting on Thursday, May 17, 2018, from 2:40 p.m. to 3:00 p.m. ET. Speakers who wish to participate in the public comment period must register in advance by no later than Friday, May 11, 2018, at 5:00 p.m. ET by emailing *NSTAC@hq.dhs.gov.* Speakers are requested to limit their comments to three minutes and will speak in order of registration. Please note that the public comment period may end before the time indicated, following the last request for comments.

FOR FURTHER INFORMATION CONTACT: Helen Jackson, NSTAC Designated Federal Officer, Department of Homeland Security, (703) 705–6276 (telephone) or *helen.jackson@hq.dhs.gov* (email).

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. Appendix (Pub. L. 92–463). The NSTAC advises the President on matters related to national security and emergency preparedness (NS/EP) telecommunications and cybersecurity policy.

Agenda: The committee will meet in an open session on May 17, 2018, receive remarks from Department of Homeland Security (DHS) leadership and other senior Government officials regarding the Government's current cybersecurity initiatives and NS/EP priorities. The meeting will include a keynote address and a debate consisting of great thinkers in cybersecurity. NSTAC members will also receive a status update on the NSTAC Cybersecurity Moonshot Subcommittee's examination of concepts related to a Cybersecurity Moonshot, which has two primary objectives: (1) Defining an ambitious but achievable outcome-focused end goal for the cybersecurity environment; and (2) defining the structure and process necessary to successfully execute against the identified end goal.

The committee will also meet in a closed session to receive a classified briefing regarding cybersecurity threats and discuss future studies based on the Government's NS/EP priorities and perceived vulnerabilities.

Basis for Closure: In accordance with 5 U.S.C. 552b(c), The Government in the Sunshine Act, it has been determined that two agenda items require closure, as the disclosure of the information discussed would not be in the public interest. The first of these agenda items, the classified briefing, will provide members with a cybersecurity threat briefing on vulnerabilities related to the communications infrastructure. Disclosure of these threats would provide criminals who seek to compromise commercial and Government networks with information on potential vulnerabilities and mitigation techniques, weakening the Nation's cybersecurity posture. This briefing will be classified at the top secret/sensitive compartmented information level, thereby exempting disclosure of the content by statute. Therefore, this portion of the meeting is required to be closed pursuant to 5 U.S.C. 552b(c)(1)(A) & (B). The second agenda item, a discussion of potential NSTAC study topics, will address areas of critical cybersecurity vulnerabilities and priorities for government. Government officials will share data with NSTAC members on initiatives, assessments, and future security requirements across public and private sector networks. The information will include specific vulnerabilities within cyberspace that affect the United States' information and communications technology infrastructures and proposed mitigation strategies. Disclosure of this information to the public would provide criminals with an incentive to focus on these vulnerabilities to increase attacks on the Nation's critical infrastructure and communications networks. As disclosure of this portion of the meeting is likely to significantly frustrate implementation of proposed DHS actions, it is required to be closed pursuant to 5 U.S.C. 552b(c)(9)(B).

Helen Jackson,

Designated Federal Officer for the NSTAC.

[FR Doc. 2018–09234 Filed 4–30–18; 8:45 am]

BILLING CODE 9110–9X–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2018–0001]

Privacy Act of 1974; System of Records

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security/U.S. Citizenship and Immigration Services proposes to modify and reissue a current Department of Homeland Security system of records, Department of Homeland Security/U.S. Citizenship and Immigration Services—012, ''United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository.'' The Citizenship and Immigration Data Repository is a mirror copy of the U.S. Citizenship and Immigration Services' major immigrant and non-immigrant unclassified benefits databases combined into a single user interface and presented in an updated searchable format on the classified network. This system of records is being updated to clarify categories of records, add the Password Issuance and Control System Identification Number as a retrievable data element, update the retention period for records maintained in CIDR; update routine use E and add routine use F to comply with new policy contained in Office of Management and Budget Memorandum M–17–12; update the record source categories, update the system manager information; and explain limitations set by law to the exemptions claimed for this system. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice and to provide further transparency as to how the system is used, in alignment with the recently republished Privacy Impact Assessment, DHS/USCIS/PIA–031(a) Citizenship & Immigration Data Repository. This modified system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before May 31, 2018. This modified system will be effective upon publication. Modified routine use E and new routine use F will be effective May 31, 2018.

ADDRESSES: You may submit comments, identified by docket number DHS–2018–0001 by one of the following methods:

• *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

• *Fax:* 202–343–4010.

• *Mail:* Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Donald K. Hawkins, *uscis.privacycompliance@uscis.dhs.gov,* 202–272–8030, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue NW, Washington, DC 20529. For privacy questions, please contact: Philip S. Kaplan, *Privacy@hq.dhs.gov,* (202) 343–1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) proposes to modify and reissue a current DHS system of records titled, ''United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository.'' USCIS is modifying this system of records notice (SORN) to add clarity as to the categories of records in the system and to provide further transparency as to how the system is used, in alignment with the recently republished Privacy Impact Assessment (PIA) for the system.

USCIS collects personally identifiable information (PII) directly from and about immigrants and nonimmigrants through applications, petitions, and other request forms for the purposes of adjudicating and bestowing immigration benefits. USCIS maintains a number of systems to facilitate these purposes including: The Computer Linked Application Information Management System (CLAIMS 3); CLAIMS 4; the Refugees, Asylum, and Parole System (RAPS); Asylum Pre-screen System (APSS); the legacy Re-engineered Naturalization Application Casework System (RNACS) (through the Enterprise Citizenship and Immigrations Services Centralized Operation Repository (eCISCOR)); Central Index System (CIS); and the Fraud Detection and National Security Data System (FDNS–DS). More information about these systems is available at *www.dhs.gov/privacy.*

USCIS developed CIDR, hosted on DHS classified networks, in order to make information from these USCIS systems available to authorized USCIS personnel for the purposes of: (1) Vetting USCIS application information for indications of possible immigration fraud, public safety, and national security concerns when classified information must be cross-referenced with unclassified data in USCIS data sets, (2) detecting possible fraud by USCIS employees, including but not limited to potential misuse of immigration information or position by USCIS employees, and responding to similar tips or referrals received from other federal agencies via classified channels, and (3) responding to requests for information (RFI), based on classified criteria, from the DHS Office of Intelligence and Analysis (I&A) and/or federal intelligence and law enforcement community members. CIDR enables authorized USCIS users to more efficiently search multiple USCIS systems from a single entry point, the results of which will be retained in CIDR. CIDR's placement on DHS classified networks allows USCIS to securely conduct searches based on classified parameters and searches based on fraud and national security concerns.

Consistent with DHS's information sharing mission, information stored in CIDR may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, USCIS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with routine uses H and I set forth in this system of records notice. Even when a valid routine use permits disclosure of information from CIDR to a third party, there may be occasions when disclosures may not be permissible because of confidentiality laws and policies that limit the sharing of information regarding individuals applying for certain immigration or non-immigration benefits.

Separately, USCIS republished a PIA, DHS/USCIS/PIA–031(a) Citizenship & Immigration Data Repository, to provide additional notice of the new functionality being incorporated into CIDR. This PIA can be found at *www.dhs.gov/privacy.*

USCIS is modifying this SORN to provide public notice of the following: (1) Categories of records have been clarified to provide notice of the information that is collected for each stated purpose; (2) the Password Issuance and Control System (PICS) Identification Number has been added as a data element by which information about USCIS users of CIDR's underlying systems may be retrieved; (3) retention period for records maintained in CIDR have been updated; (4) routine use E has been updated and routine use F has been added to comply with requirements set forth by OMB Memorandum M–17–12, ''Preparing for and Responding to a Breach of Personally Identifiable Information,'' (Jan. 3, 2017); (5) record source categories have been updated to provide further transparency as to the data sources that will be incorporated into CIDR; (6) system manager information has been updated; and (7) exemptions claimed for this system remain in effect. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Previously, DHS issued a final rule published on December 28, 2010 (75 FR 81371) at 6 CFR part 5, Appendix C, paragraph 53 exempting this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). This rule remains in effect. To the extent USCIS maintains a record received from a law enforcement system that has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions. This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework, governing 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. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides a statutory right to covered persons 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 DHS/USCIS–012 Citizenship and Immigration Services Data Repository (CIDR) System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this

system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository.

SECURITY CLASSIFICATION:

Unclassified and Classified.

SYSTEM LOCATION:

Records are maintained at the USCIS Headquarters at 111 Massachusetts Ave. NW, Washington, DC.

SYSTEM MANAGER:

Chief, Program Management Office, Fraud Detection and National Security Directorate, USCIS, *FDNSCommunications@uscis.dhs.gov,* 111 Massachusetts Avenue NW, Washington, DC, 20529.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Immigration and Nationality Act, sections 101 and 103, as amended (8 U.S.C. 1101 and 1103), and the regulations issued pursuant thereto; sec. 453 and 454 of the Homeland Security Act of 2002 (Pub. L. 107–296); Executive Order 12958, and as amended; E.O. 13388; and E.O. 12333, and as amended.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to (1) vet USCIS application information for indications of possible immigration fraud, public safety, and national security concerns when classified information must be cross-referenced with unclassified data in USCIS data sets, (2) detect possible fraud and misuse of immigration information or position by USCIS employees, for personal gain or by coercion when USCIS receives tips or referrals from other federal agencies via classified channels, and (3) respond to RFIs from the DHS I&A and/or the federal intelligence and law enforcement community members that are based on classified criteria.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: persons who have filed (for themselves or on the behalf of others) applications or petitions and other request forms for immigration benefits under the Immigration and Nationality Act, as amended, or who have submitted fee payments or received refunds from such applications or petitions; current, former and potential (*e.g.,* fiancé) family members of applicants/petitioners; persons who complete immigration forms for applicants and petitioners (*e.g.,* attorneys, interpreters, form preparers); names of applicant's employer; and individuals referred to USCIS for reasonable fear and credible fear screenings. Additionally, CIDR maintains information on USCIS personnel who have used CIDR or the underlying USCIS systems included in CIDR.

CATEGORIES OF RECORDS IN THE SYSTEM:

CIDR receives information on individuals whose information is maintained in USCIS source systems, USCIS personnel who accessed the underlying source systems, and Federal Government employees who submit a RFI or other classified correspondence to USCIS. CIDR will not modify the source data contained in the underlying systems. Information collected about individuals may include, but is not limited to:

- Names (and types of individuals): First name, last name, middle name, and any aliases of the applicant/petitioner/requestor, beneficiary, or family members. USCIS also collects names of sponsors, form preparers, attorneys, and designated representatives.
- Immigration Status: Status and status expiration dates relating to the benefit applicant/petitioner/requestor, beneficiary, family member, and sponsor.
- Travel Information: Destination in the United States, port of entry, days spent outside the United States, dates of entry, arrival and departure dates, passport number, passport place of issue, passport issue date, passport expiration date, travel document number, travel document country of issue, and travel document expiration date.
- Marital Status and History: Current and former marital status of the benefit applicant/petitioner/requestor or beneficiary, the dates of and place of marriages or terminations, and the reason for termination.
- Addresses: Benefit applicants/petitioners/requestors, beneficiaries, family members, sponsors, attorneys, representatives. For certain benefits, a requestor or beneficiary can provide both a home address and an alternative mailing address.
- Telephone and Facsimile Numbers: Benefit applicants/petitioners/requestors, beneficiaries, family members, sponsors, household members, attorneys, and representatives.
- Email Addresses: Benefit applicants/petitioners/requestors, beneficiaries, family members, attorneys, and representatives.
- Dates of Birth and Age: Benefit applicants/petitioners/requestors, beneficiaries, sponsors, and family members.
- Unique Identifying Numbers: Alien Numbers (A-Numbers), Social Security numbers (SSN), USCIS Online Account Numbers, receipt numbers, and other identifying numbers of benefit applicants/petitioners requestors, beneficiaries, family members, and sponsors.
- Citizenship/Nationality: Benefit applicants/petitioners/requestors, beneficiary, or family member's country of citizenship or nationality, and country of birth.
- Gender: Benefit applicants/petitioners/requestors, beneficiaries, and family members.
- Personal Characteristics: Benefit applicants/petitioners/requestors or beneficiary's hair color, eye color, height, weight, race, and ethnicity.
- Information about the attorney, representative, form preparer, or interpreter: Full name, business or organization, mailing address, email address, phone number, fax number, signature, language spoken, relationship to the benefit requestor or beneficiary (if applicable). USCIS also collects Attorney Bar Number or equivalent, Bar Membership, Accreditation Date, Board of Immigration Appeals Representative Accreditation Expiration Date, and Law Practice Restriction Explanation.
- Biometrics: Benefit applicants/petitioners/requestors or beneficiary's biometric images such as press-print, photograph, details about those images (*e.g.,* capture date), and signature of benefit requestor, beneficiary, interpreter, and representative.
- Card Data: Details about USCIS-issued cards (*e.g.,* Employment Authorization Document and the Permanent Resident Cards) for approved applications such as card serial number, Radio-frequency identification (RFID) data, production site, production status, and time/date stamp of cards.
- Tax and Financial Information: Tax identification numbers, and financial information (check information, bank account numbers, credit card numbers (the last four digits only) and other tax and financial information information).
- Results of Background, Identity and Security Checks: Date of the background check, whether the check returned any derogatory results, whether those results were resolved, and expiration date of the results.
- Certifying Agency Information (if applicable): Agency name, certifying official name, title of certifying official,

address, phone, fax, agency type, case status, agency category, case number, FBI Number, or State Identification (SID) Number.

• Medical Information: Collected and used to establish that an applicant is not inadmissible to the United States on public health grounds, as well as in support of a request for an accommodation during an interview. Such information may indicate alcoholism, declaration of incompetence, or family medical history.

• Employment Information: Collected and used to determine the benefit requestor and beneficiary's eligibility. Such information includes place and address of employment/occupation, type of work, employer name, length of employment, spouse's employment.

• Military and Selective Service Information: Collected and used to verify that the benefit requestor or beneficiary has registered with Selective Service as required by law. Such information includes Selective Service number, date of registration, application for military exemption, military branch, and willingness to bear arms for the United States of America.

• Information Regarding Organization Membership or Affiliation: Collected and used to determine whether the applicant poses a security threat to the United States or individuals or has participated in activities that may disqualify him or her for a requested benefit. Such information includes an applicant's organization memberships and affiliations (*i.e.,* organizations, associations, clubs, foundations, parties, societies, or similar groups; communist party membership; totalitarian party membership; terrorist organization membership).

• Criminal History or Involvement and Moral Character Issues: Collected and used to assess whether the applicant meets the standards contained in the INA. Such information includes an applicant's criminal history, involvement in criminal activities, and information regarding moral character.

• Case Processing Information: Date USCIS received or filed benefit requests; benefit request status; location of record; other control number when applicable; fee receipt data; status of USCIS appointments and interviews; date of issuance of a notice; and whether the benefit request form was referred to FDNS for review.

• Final Decision: Final notice to the benefit requestors, beneficiary, and/or the representative on record, approval/denial code, etc.

CIDR maintains information on USCIS personnel who use the underlying USCIS systems included in CIDR as well as CIDR itself, which includes, but is not limited to:

• System audit logs, including PICS Identification Numbers assigned to users of the underlying USCIS systems;

• Records of searches, analyses, correspondence, and outputs generated by USCIS personnel in response to a classified request for USCIS immigrant and non-immigrant data;

CIDR does not collect or track specific data elements concerning personnel of other federal agencies; however, the classified correspondence associated with background checks or RFIs is maintained in CIDR in a searchable format. These documents may include contact information such as names, agency, title, work addresses, or phone numbers.

RECORD SOURCE CATEGORIES:

Records are obtained from the following systems of records:

USCIS Systems:

• DHS/USCIS–007 Benefit Information System, 81 FR 72069 (October 19, 2016), which corresponds to the following USCIS databases:

○ CLAIMS 3, case tracking for all benefits except refugee status, asylum, and naturalizations;

○ CLAIMS 4, case tracking for naturalization and citizenship benefits; and

○ RNACS, interim legacy system used to support naturalization processing in the period between the termination of Naturalization Application Casework System and the deployment of CLAIMS 4.

• DHS/USCIS–006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012), which covers the following database:

○ Fraud Detection and National Security Data System (FDNS–DS, screening and case management system used to record requests and case determinations involving benefit fraud, public safety, and national security concerns); and

○ Service Center Computer-Linked Application Information Management System (SCCLAIMS), a mirror copy of CLAIMS 3 data, used to facilitate searches.

• DHS/USCIS/ICE/CBP–001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017), which covers the following USCIS database:

○ Central Index System (CIS, contains status information on applicants/petitioners seeking immigration benefits)

• DHS/USCIS–010 Asylum Information and Pre-Screening, 80 FR 74781 (November 30, 2015), which corresponds to RAPS/APSS. RAPS, is a case management system that tracks applications for asylum pursuant to section 208 of the Immigration and Naturalization Act (INA) and applications for suspension of deportation or special rule cancellation of removal pursuant to Nicaraguan Adjustment and Central American Relief Act (NACARA) section 203 of the INA. APSS is a case management system that tracks the processing of ''Credible Fear'' and ''Reasonable Fear'' cases by Asylum staff.

• DHS/USCIS–017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (October 19, 2016), which covers the collection and use of refugee applicants, refugee derivatives, and follow-to-join applicants.

DHS Intelligence and Analysis System:

• DHS/IA–001, Office of Intelligence and Analysis (I&A) Enterprise Records System, 73 FR 28128 (May 15, 2008).

DHS-Wide System:

• DHS/ALL–004 General Information Technology Access Account Records System of Records, 77 FR 70792 (November 27, 2012).

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

Information in this system of records contains information relating to persons who have pending or approved benefit requests for special protected classes and should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under the confidentiality statutes, regulations, or policies applicable to that information. For example, information relating to persons who have pending or approved benefit requests for protection under the Violence Against Women Act, Seasonal Agricultural Worker or Legalization claims, Temporary Protected Status, and information relating to nonimmigrant visas. These confidentiality provisions do not prevent DHS from disclosing information to the U.S. Department of Justice (DOJ) and Offices of the United States Attorney as part of an ongoing criminal or civil investigation.

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

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting

litigation or in proceedings before any court, adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

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

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection 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.

G. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

H. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To a federal, state, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

DHS/USCIS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by any of the data elements listed above or a combination thereof. This may include, name, date of birth, Alien Number, SSN, USCIS Online Account Number, Receipt Number, and PICS Identification Number. Additionally, records may be retrieved by the output of USCIS's search, analysis, and response to classified requests for USCIS data.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

CIDR does not retain the replicated data sets from the underlying USCIS data systems, to include CLAIMS 3, CLAIMS 4, RAPS, APSS, RNACS, and CIS, and the associated audit trails of DHS personnel using the systems. The data supplied by these systems are retained by those systems in accordance with their own retention schedules. CIDR simply mirrors these data sets. Information will be removed from CIDR after it has been removed in the source system.

USCIS is working with the NARA to develop a records retention schedule to cover the records retained in CIDR, such as classified background check responses. USCIS proposes to retain background check related records 100 years from the date of birth. The 100-year retention rate comes from the length of time USCIS may interact with a customer. Further, retaining the data for this period of time will enable USCIS to fight identity fraud and misappropriation of benefits. This proposed records retention schedule is consistent with the approved NARA Disposition Authority Number DAA–0563–2013–0001–0005.

Records used as part of a benefit determination are maintained in the Alien File and processed in the respective USCIS case management system. The A-File records are permanent whether in hard copy or electronic form. USCIS transfers the A-Files to the custody of NARA 100 years after the individual's date of birth. Electronic benefits information is archived and disposed of in accordance with NARA-approved retention schedule for the respective USCIS systems.

CIDR retains a record of the classified search request, the results of the request, and a log of these activities for up to 25 years. These are maintained for a minimum of five years in accordance with Director of Central Intelligence Directive (DCID) 6/3. Classified data will be maintained for the period of time required by the originating classification authority.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/USCIS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. USCIS has imposed strict controls 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 those 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:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). However, each request for information within CIDR will be reviewed to

determine whether or not the record within CIDR meets the requirements of the exemptions and, as appropriate, to disclose information that does not meet the requirements. This does not prevent the individual from gaining access to his records in the source systems noted below. Persons may seek access to records maintained in the source systems that feed into CIDR, currently CLAIMS 3, and in future releases, CLAIMS 4, RAPS, APSS, RNACS, and CIS.

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 in writing to the Chief Privacy Officer and to the USCIS FOIA/Privacy Act (PA) Officer whose contact information can be found at *http://www.dhs.gov/foia* under ''Contacts Information.'' If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about an individual may be available under the Freedom of Information Act.

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 6 CFR part 5. The individual must verify his or her identity, meaning that the individual must provide his or her 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. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, *http://www.dhs.gov/foia* or 1–866–431–0486. In addition, the individual should:

- Explain why the individual believes the Department would have information on him or her;
- Identify which component(s) of the Department the individual believes may have the information about you;
- 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's request is seeking records pertaining to another living individual, he or she must include a statement from that individual certifying his/her agreement for the individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see ''Record Access Procedures'' above. Any individual, regardless of immigration status, may file a request to access his or her information under the FOIA. Throughout the benefit determination process and prior to USCIS making a determination to deny a benefit request, USCIS provides individuals with the opportunity to address and correct the information.

NOTIFICATION PROCEDURES:

See ''Record Access Procedures.''

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2).

Additionally, many of the functions in this system require retrieving records from law enforcement systems. When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY:

DHS/USCIS–012, United States Citizenship and Immigration Services—012 Citizenship and Immigration Data Repository, 75 FR 54642 (September 8, 2010). Final Rule for Privacy Act Exemptions, 75 FR 81371 (December 28, 2010).

Philip S. Kaplan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2018–09235 Filed 4–30–18; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2018–0009]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, ''Department of Homeland Security/United States Coast Guard-032 Asset Logistics Management Information System (ALMIS) System of Records.'' This system of records allows the DHS/United States Coast Guard (USCG) to collect and maintain records on the maintenance, mission scheduling, and logistics for USCG aviation and surface (boats) assets. This newly established system will be included in the DHS inventory of record systems.

DATES: Submit comments on or before May 31, 2018. This new system will be effective upon publication. Routine uses will be effective May 31, 2018.

ADDRESSES: You may submit comments, identified by docket number DHS–2018–0009 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov*. Follow the instructions for submitting comments.
- *Fax:* 202–343–4010.
- *Mail:* Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.

Instructions: All submissions received must include the agency name and docket number DHS–2018–0009. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT:

For general questions, please contact: Brian P. Burns, (202) 475–3507, *Brian.P.Burns@uscg.mil,* Acting Privacy Officer, Commandant (CG–6), United States Coast Guard, Mail Stop 7710, Washington, DC 20593.

For privacy questions, please contact: Philip S. Kaplan, (202) 343–1717, *privacy@hq.dhs.gov,* Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528–0655.