**DEPARTMENT OF HOMELAND SECURITY**

[Docket No. DHS-2018-0003]

**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 consolidate two legacy systems of record, Department of Homeland Security/U.S. Citizenship and Immigration Services-002 Background Check Service and Department of Homeland Security/U.S. Citizenship and Immigration Services-003 Biometric Storage System into the new DHS system of records titled, "Department of Homeland Security/U.S. Citizenship and Immigration Services-018 Immigration Biometric and Background Check System of Records." This system of records notice (SORN) allows the DHS U.S. Citizenship and Immigration Services (USCIS) to collect and maintain biographic, biometric, and background check records on applicants, petitioners, sponsors, beneficiaries, or other individuals in connection with a benefit request. USCIS uses biometric and associated biographic information to verify identity, conduct criminal and national security background checks against internal and external government systems, and to support domestic and foreign data sharing agreements. The categories of individuals, categories of records, and the routine uses of these legacy systems of records notices have been consolidated and updated to better reflect the Department's biometric and biographic criminal background checks; identity

enrollment, verification, and resolution; document production record systems; and data sharing efforts.

Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the *Federal Register*. This new system will be included in DHS's inventory of record systems.

**DATES:** Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This system will be effective upon publication. Routine uses will become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2018-0003 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, D.C. 20528-0655.

*Instructions:* All submissions received must include the agency name and docket number DHS-2018-0003 for this notice. 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: Donald K. Hawkins, (202) 272-8030, USCIS.PrivacyCompliance@uscis.dhs.gov, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue N.W., Washington, D.C. 20529. 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, D.C. 20528-0655.

**SUPPLEMENTARY INFORMATION:**

I. Background

DHS USCIS has relied on two preexisting DHS/USCIS Privacy Act SORNs for the maintenance of USCIS biometric and background check records: "DHS/USCIS 002 Background Check Service," 72 FR 31082 (June 5, 2007), and "DHS/USCIS-003 Biometric Storage System," 72 FR 17172 (April 6, 2007). Such records will be covered by one new system of records named "DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records." USCIS processes and adjudicates most immigration benefit requests and other immigration request forms (e.g., applications and petitions) for DHS. This new system of records notice consolidates and covers all of USCIS's biometric and associated biographic information it collects pursuant to that mission. The purpose of this system is to verify identity and conduct criminal and national security background checks in order to establish an individual's eligibility for an immigration benefit or other request, and support domestic and international data sharing efforts. USCIS determines eligibility by capturing biometric and associated biographic data from benefit requestors, beneficiaries, and other categories of individuals to facilitate three key operational functions: (1) verify an individual's identity; (2) conduct criminal

and national security background checks; and (3) produce benefit cards and documents as a proof of benefit.

Most individuals who file benefit requests for themselves or on the behalf of others (i.e., petitioner, applicants, beneficiaries, and requestors) are subject to background, identity, and security checks to ensure eligibility for the requested benefit. Other individuals in connection with immigration benefit requests or other requests (i.e., household members, sponsors) may also be subject to certain background, identity, and security checks. The biometric collection process begins with the capture of biometric data at an authorized biometric capture site, including USCIS offices, Application Support Centers, or U.S. consular offices and military installations abroad. USCIS requires applicants, petitioners, sponsors, beneficiaries, or other individuals in connection of a benefit request to submit their biometrics along with associated biographic information to USCIS for background, identity, and security checks. The types of background checks USCIS conducts vary by the benefit or request type. Standard background checks may include, but are not limited to:

**Biometric based checks:**

- Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) Biometric Check;
- DHS Office of Biometric and Identity Management (OBIM) Automated Biometric Identification System (IDENT) Biometric Check;
- Department of Defense (DoD) Automated Biometric Identification System (ABIS) Biometric Check;

**Biographic name-based checks:**

- FBI Central Records System (CRS) and Universal Index (UNI) Name Check;
- U.S. Customs and Border Protection (CBP) TECS Name Checks;
- Department of State (DOS) Consular Lookout and Support System (CLASS); and
- DOS Security Advisory Opinion (SAO).

USCIS may also perform interagency checks with intelligence community partners for certain benefits. The results of these checks are used to inform eligibility determinations, which will result in the approval or denial of a benefit. If fraudulent activity, criminal activity, or potential threats to public safety or national security are detected as a result of the biometric or name check, information may be referred to the USCIS Fraud Detection and National Security Directorate (FDNS) or appropriate law enforcement agencies for further review. These law enforcement agencies include U.S. Immigration and Customs Enforcement (ICE), CBP, FBI, or other federal, state, local, tribal, foreign, or international law enforcement agencies. USCIS may also conduct additional background and security checks against other federal, international, state, and local systems to verify the identity of the individual as part of the eligibility determination for a benefit or request, as appropriate.

USCIS sends biometric, associated biographic, and encounter-related data to IDENT to conduct biometric searches against the system. IDENT is the central DHS-wide information technology system for enrollment, storage, and processing of biometric and associated biographic information. IDENT is maintained for the purposes of national security, law enforcement, immigration and border management, intelligence, and credentialing (e.g., background investigations for national security positions and certain

positions of public trust), as well as for other administrative uses (e.g., providing associated testing, training, management reporting, or planning and analysis). When an authorized request is received by OBIM, the program management office for IDENT, analysts search IDENT for biometric matches and assign matches as new encounters into IDENT on behalf of USCIS. Consistent with this SORN and other SORNs governing different biometric data sets in IDENT, USCIS biographic and biometric information from IDENT may be shared with federal, state, local, tribal, foreign, and international agencies for national security, law enforcement, criminal justice, immigration and border management, and intelligence purposes. In addition, information from IDENT may also be shared for background investigations for national security positions and certain positions of public trust in accordance with statutory and regulatory restrictions on disclosure.

**International Biometric Sharing Initiatives**

This system of records supports the biometric vetting capability outlined in data sharing agreements between DHS and certain foreign partners. USCIS may send and receive biometric requests to and from certain foreign partners through IDENT in support of its immigration mission and applicable laws. The purpose of these data sharing initiatives is to enhance the cooperation between the United States and foreign partners to prevent terrorism, including terrorist travel; prevent serious crime and other threats to national security and public safety; assist in the administration and enforcement of immigration laws; and provide the foreign partner with appropriate information for its consideration when adjudicating requests for immigration benefits including, but not limited to, asylum or refugee status. Through international sharing agreements, USCIS

may share biometric and associated biographic information stored in IDENT, which it collected in determining suitability for an immigration benefit, with foreign partners. DHS does not permit third party disclosure without prior approval.

**Document Production**

Once the adjudication of certain immigration benefits are complete, USCIS creates official, personalized and secure identity documents to certify the grant of the requested benefit. The secure identification documents USCIS produces and issues are high-quality and state-of-the-art, incorporating tamper-resistant, machine-readable, and biometrically-enabled technologies designed to withstand document counterfeiting efforts, alteration, or efforts employed to commit fraud.

Information stored in the DHS/USCIS-018 IBBC System of Records 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, DHS/USCIS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing an NPRM to exempt this system of records from certain provisions of the Privacy Act elsewhere in the *Federal Register*. This new system of records 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 under 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 statutory rights to covered persons to request 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-018-Immigration Biometric and Background Check (IBBC) 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:** DHS/ USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records.

**SECURITY CLASSIFICATION:** Unclassified and classified. The data may be retained on classified networks but this does not change the nature and character of the data until it is combined with classified information.

**SYSTEM LOCATION:** DHS/USCIS maintains records in DHS-approved data centers in the Washington, D.C., metropolitan area. Backups are maintained offsite. IBBC will be accessible world-wide from all USCIS field offices, service centers, and Application Service Centers that are part of the DHS Network. Paper files are located at USCIS Headquarters in Washington, D.C. and in DHS/USCIS service centers, domestic and

international field offices, and other USCIS facilities. USCIS stores biometric records in the DHS biometrics repository, OBIM IDENT.

DHS/USCIS replicates records from the operational IT systems and maintains them in other IT systems connected on the DHS unclassified and classified networks.

**SYSTEM MANAGER(S):** Associate Director, Immigration Records and Identity Services, BD.systems@uscis.dhs.gov, U.S. Citizenship and Immigration Services, Department of Homeland Security, 111 Massachusetts Avenue, N.W., Washington, D.C. 20529.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 8 U.S.C. 1101 and 1103; 8 C.F.R. 103.16(a); and 8 C.F.R. 103.2(b)(9).

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to assist USCIS with determining an individual's eligibility for an immigration benefit request or other USCIS requests. USCIS captures biographic and biometric data from applicants, petitioners, sponsors, beneficiaries, or other individuals to facilitate three key operational functions: (1) enroll, verify, and manage an individual's identity; (2) conduct criminal and national security background checks; and (3) produce benefit cards/documents as a proof of benefit. Also, the purpose of this system is to (4) support data sharing initiatives between DHS components, other U.S. Government agencies and foreign partners in order to prevent terrorism, including terrorist travel; prevent serious crime and other threats to national security and public safety; and assist in the administration and enforcement of immigration laws.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Categories of individuals covered by this system include:

- Persons who have filed on their own behalf, or on the behalf of others, applications or petitions for immigration benefits or other requests under the Immigration and Nationality Act (INA) (i.e., applicants, petitioners, and beneficiaries), as amended;
- Current, former, and potential derivative family members of benefit requestors;
- Affiliated persons who have a clearly articulated rational connection to the request, applicant, petitioner, or beneficiary, that may have an impact on the adjudication process of a request;
- Associates whose information is voluntarily provided by the applicant as part of the family tree, and which include points of contact in the United States and other individuals with whom the applicant associates (i.e., household members, sponsors);
- Attorneys and representatives recognized by USCIS and/or accredited by the Board of Immigration Appeals (Representatives); and
- All individuals who meet the definition of an adult member of the household, 8 C.F.R. 204.3(b) or 8 C.F.R. 204.301; and/or any other individual whose presence in the applicant's or petitioner's residence is relevant to the prospective adoptive parent(s)'s suitability to adopt overseas.

**CATEGORIES OF RECORDS IN THE SYSTEM:** This system covers biographic, biometric, unique machine-generated identifiers, encounter-related data, criminal and national security background check results, and card production information.

*Biographic information may include:*

- Full name;

- Aliases;
- Other names;
- Date of birth;
- Place of birth;
- Country of Citizenship/Nationality;
- Current and previous immigration status;
- Mailing and physical address;
- Phone number;
- Employment status;
- Travel Document Numbers (i.e., passport numbers, I-94 number);
- Travel Document Information (i.e., country of issuance, nationality, date of issuance, expiration date);
- Case Type (i.e., refugee claimant, identity investigation, absconder, visa applicant);
- Filing date;
- Filing determination;
- Reason for filing determination;
- Gender;
- Height;
- Weight;
- Eye color;
- Hair color;

- Race/Ethnicity; and
- Unique Identifying Numbers, including, but not limited to, Alien Registration Number (Alien Number), Receipt Number, Social Security number (SSN), and USCIS Online Account Number.

*Biometric information may include:*

- Biometric images (including, but not limited to: photographs/facial images, fingerprint images, iris images, voice samples, and signatures); and
- Details about images (i.e., capture date, reason fingerprinted, and location).

*Encounter information may include*:

- Scan of marked travel document page;
- Foreign partner point of contact information;
- Watchlist indicator, indicator of derogatory information, or reason for alert;
- Arrival, Departure, and/or Removal information (date and location);
- Transaction Control Numbers Associated with FBI fingerprint checks;
- Date/time of submission;
- Type of immigration form or non-biometric encounter;
- Date of immigration form or non-biometric encounter;
- Query results (match or no match);
- Error code; and
- Transaction Identifier Data (i.e., sending organization; timestamp; date; transaction type; case type; priority level; message origin; message destination; reference numbers (requesting participants subject specific reference number; or

requesting participants event specific reference number)); workstation; reason fingerprinted, such as entry, visa application, credentialing application, or apprehension; and any available encounter information, including an IDENT-generated encounter identification number (EID)).

*Background Check information may include:*

- Results of criminal and national security background checks (i.e., positive or negative response; and positive responses are generally accompanied with the individual's criminal history and additional information explaining the results of the response); Unique Biometric Identifier (i.e., Fingerprint Identification Number (FIN) and Universal Control Number (formerly known as FBI Number)); and
- Logs associated with the requests of background checks, which may include requesting location and requesting person.

*Document Production information may include*:

- Identifying Transactional Information (i.e., transaction control number, book number);
- Biographical Information used for Document Production;
- Document Production Status;
- Benefit Card/Document Type;
- Class of Admission;
- Document Serial Number;
- Radio Frequency Identification (RFID) with USCIS Issued Document;
- Machine-readable Barcode;
- Production Site;

- Production Status; and
- Document Issuance Time/Date and Expiration Date.

**RECORD SOURCE CATEGORIES:** Records are obtained from the categories of individuals included in this SORN. Information contained in this system may also be supplied by DHS, other U.S. Federal, state, tribal, or local government agencies, foreign government agencies, and international organizations. USCIS personnel may input information as they process a case, including information from internal and external sources, and to verify whether a benefit requestor or family is eligible for the benefit requested. Records covered by other systems of records (or their successor systems) that are ingested and covered by this SORN include the following:

1. DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017);
2. DHS/USCIS-005 Intercountry Adoptions Security, 81 FR 78614 (Nov. 8, 2016);
3. DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012);
4. DHS/USCIS-007 Benefit Information System, 81 FR 72069 (Oct. 19, 2016);
5. DHS/USCIS-010 Asylum Information and Pre-Screening, 80 FR 74781 (Nov. 30, 2015);
6. DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (Oct. 19, 2016);
7. DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008);

8. DHS/ICE-011-Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016);
9. DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007);
10. DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018);
11. JUSTICE/FBI-002 The FBI Central Records System, 82 FR 24147 (May 25, 2017), and prior history (https://www.justice.gov/opcl/doj-systems-records);
12. JUSTICE/FBI-009 The Next Generation Identification (NGI) System, 81 FR 27283 (May 5, 2016), and 82 FR 24151 (May 25, 2017);
13. STATE-05 Overseas Citizens Services Records and Other Overseas Records, 81 FR 62235 (Sept. 8, 2016);
14. STATE-26 Passport Records, 80 FR 15653 (March 24, 2015);
15. STATE-39 Visa Records, 77 FR 65245 (Oct. 25, 2012);
16. STATE-59 Refugee Case Records, 77 Fed. Reg. 5865 (Feb. 6, 2012);
17. ODNI/NCTC–008 National Counterterrorism Center Terrorism Analysis Records, 72 FR 73895 (Dec. 28, 2007);
18. DoD/A0025-2 Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009);
19. DoD/A0025-2 PMG (DFBA) Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015); and
20. DoD/A0025-2a Defense Biometric Identification Records System, 74 FR 17840 (April 17, 2009).

**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 certain persons who have pending or approved benefit requests for special protected class status 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 applied for asylum or refugee status, have pending or approved benefit requests for protection under the Violence Against Women Act, Seasonal Agricultural Worker or Legalization claims, the Temporary Protected Status of an individual, and information relating to certain nonimmigrant visas. These confidentiality provisions do not prevent DHS from disclosing information to the Department of Justice (DOJ) and Offices of the United States Attorneys 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 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. secs. 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 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 appropriate Federal, state, local, tribal, territorial, or foreign governments, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates.

J. To a former employee of DHS, in accordance with applicable regulations, for purposes of: responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority; or facilitating communications with a former

employee that may be necessary for personnel-related or other official purposes when DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To a coroner, in accordance with applicable law and regulations, for purposes of affirmatively identifying a deceased individual (whether or not such individual is deceased as a result of a crime).

L. To a Federal, state, or local government agency seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law

M. To an appropriate domestic government agency or other appropriate authority for the purpose of providing information about an individual who has been or is about to be released from DHS custody who, due to a condition such as mental illness, may pose a health or safety risk to himself/herself or to the community. DHS will only disclose information about the individual that is relevant to the health or safety risk they may pose and/or the means to mitigate that risk (e.g., the individuals need to remain on certain medication for a serious mental health condition).

N. To foreign governments for the purpose of coordinating and conducting the removal of individuals to other nations under the INA; and to international, foreign, and intergovernmental agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

O. To DOJ FBI for the purpose of conducting name and fingerprint background checks in order to verify the identity of an individual and generate information used to grant or deny an immigration benefit request or other request.

P. To U.S. Department of State for the purpose of conducting biographic and biometric based searches for identity verification in order to process requests for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements; or when DOS requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications.

Q. To U.S. Department of Defense for the purpose of biometric background checks to verify the identity of an individual and generate information used to grant or deny an immigration benefit request or other request.

R. To the Office of the Director of National Intelligence National Counterterrorism Center (ODNI/NCTC) and other Federal and foreign government intelligence or counterterrorism agencies when USCIS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

S. To an individual's prospective or current employer to the extent necessary to determine employment eligibility (for example, pursuant to the Form I-140, *Immigrant Petition for Alien Worker*).

T. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of

DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

**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, but is not limited to, name, date of birth, Alien Number, SSN, USCIS Online Account Number, and Receipt Number.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** USCIS retains the records 100 years from the date of birth of the individual in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005. USCIS collects and uses the information to verify the identity of the individual and support the background check process. 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.

USCIS generates secure identification documents to communicate adjudication decisions to the mailing address on file for the benefit requestor or his or her legal representative. USCIS systems that generate cards and documents retain data 10 years from the date of record creation in accordance with NARA Disposition Authority Number DAA-0566-2016-0014. Proof of benefits sent to the benefit requestor and

returned to USCIS are retained by USCIS for up to one year in accordance with NARA Disposition Authority Number DAA-0566-2014-0005.

**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, and consequently the JRA if applicable, because it may interfere with ongoing investigations and law enforcement activities. However, DHS will consider individual requests to determine whether or not information may be released. Thus, 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 Headquarters or component's FOIA 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 FOIA Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about the 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 individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first 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 FOIA Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why the individual believe the Department would have information on him or her;
- Identify which component(s) of the Department the individual believes may have the information about him or her;
- 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, the first individual must include a statement from that individual certifying his/her agreement for the first individual to access his/her records.

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

**CONTESTING RECORD PROCEDURES:** For records covered by the Privacy Act or covered JRA records, see "Records 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, pursuant to Secretary's delegation number 15002 to the Director of USCIS to conduct certain law enforcement activities, when necessary to protect the national security and public safety, pursuant to 5 U.S.C. 552a(j)(2), is proposing to exempt this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). When a record received from another system has been 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-002 Background Check Service, 72 FR 31082 (June 5, 2007);

DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 6, 2007).

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2018-16138 Filed: 7/30/2018 8:45 am; Publication Date: 7/31/2018]