section 207(c)(2), and 208(c) of the INA (8 U.S.C. 1157 and 1158) for an asylee or refugee to request accompanying or following-to-join benefits for his or her spouse and unmarried minor child(ren).

• OMB No. 1615–0038—Form I–751, Petition to Remove Conditions on Residence: Collection of data through this form is authorized by INA section 216, 8 U.S.C. 1186(a); 8 CFR part 216.

• OMB No. 1615–0045—Form I–829, Petition by Entrepreneur to Remove Conditions on Permanent Resident Status: Collection of data through this form is authorized by INA section 203(b)(5), 8 U.S.C. 1153, and INA section 216(a),8 U.S.C. 1186(b)].

Applicant information is collected to maintain a record of persons applying for specific immigration and other travel benefits, and to determine whether these applicants are eligible to receive the benefits for which they are applying. The information provided through DHS forms is also analyzed—along with other information that the Secretary of Homeland Security determines is necessary, including information about other persons included on the DHS forms —against various security and law enforcement databases to identify those applicants who may pose a security risk to the United States. To obtain approval for a collection that meets the conditions of this generic clearance, a standardized form will be submitted to OMB along with supporting documentation (*e.g.,* a copy of the updated application form). OMB will grant approval only if the agency demonstrates the collection of information complies with the specific circumstances laid out in this supporting statement.

Confidentiality

No assurance of confidentiality is provided. All data submitted under this collection will be handled in accordance with applicable U.S. laws and DHS policies regarding personally identifiable information.

• Public Law 107–347, ''E-Government Act of 2002,'' as amended, Section 208 [44 U.S.C. 3501 note].

• Title 5, United States Code (U.S.C.), Section 552a, ''Records maintained on individuals'' [The Privacy Act of 1974, as amended].

• Title 6, U.S.C., Section 142, ''Privacy officer.''

• Title 44, U.S.C., Chapter 35, Subchapter II, ''Information Security'' [The Federal Information Security Modernization Act of 2014 (FISMA)].

• DHS Directive 047–01, ''Privacy Policy and Compliance'' (July 25, 2011).

• DHS Instruction 047–01–001, ''Privacy Policy and Compliance'' (July 25, 2011).

• Privacy Policy Guidance Memorandum 2008–01/Privacy Policy Directive 140–06, ''The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.'' (December 29, 2008).

• Privacy Policy Guidance Memorandum 2017–01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information. (April 25, 2017).

• Refugees and asylees are protected by the confidentiality provisions of 8 CFR 208.6; 8 U.S.C. 1103. Aliens in TPS status have the confidentiality protections described in 8 CFR 244.16; 8 U.S.C. 1254a(c)(6). There are no confidentiality assurances for other aliens applying for the benefit.

• The system of record notices associated with this information collection are:

○ DHS/USCIS/ICE/CBP–001—Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR 43556 (all USCIS forms).

○ DHS/USCIS–007—Benefits Information System, October 19, 2016, 81 FR 72069 (Forms N–400, I–131, I–192, I–485, I–590, I–730, I–751, I–829).

○ DHS/USCIS–010—Asylum Information and Pre-Screening System of Records November 30, 2015, 80 FR 74781 (Form I–589).

○ DHS/CBP–006—Automated Targeting System, May 22, 2012, 77 FR 30297 (Form I–192).

○ DHS/USCIS–017—Refugee Case Processing and Security Screening Information System of Records October 19, 2016, 81 FR 72075 (Forms I–730).

○ DHS/CBP—Electronic Visa Update System (EVUS) System of Records, September 1, 2016, 81 FR 60371 (EVUS Form); Final Rule for Privacy Exemptions, November 25, 2016, 81 FR 85105.

○ DHS/CBP–009—Electronic System for Travel Authorization (ESTA), September 2, 2016, 81 FR 60713 (ESTA Form); Final Rule for Privacy Act Exemptions, August 31, 2009 74 FR 45069.

○ DHS/CBP–016—Nonimmigrant Information System March 13, 2015, 80 FR 13398 (Form I–94W).

○ DHS/USCIS–015—Electronic Immigration System-2 Account and Case Management System of Records April 5, 2013 78 FR 20673 (Form I–131).

This is a new generic clearance. This request will be submitted to the Office of Management and Budget, Office of Information and Regulatory Affairs for review and approval as required by the Paperwork Reduction Act. This new collection is to meet the intent of E.O. 13780 (Section 5) to establish screening and vetting standards to assess an alien's eligibility to travel to, be admitted to, or receive an immigration-related benefit from DHS. This information will be used to validate an applicant's identity and determine whether entry to the U.S. or an immigration benefit for an individual poses a law enforcement or national security risk to the United States.

DHS is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submissions of responses.

Analysis

Agency: Department of Homeland Security DHS.

Title: Generic Clearance for the Collection of Certain Information on Immigration and Foreign Travel Forms.

OMB Number: 1601–NEW.

Frequency: On Occasion.

Affected Public: Individuals.

Number of Respondents: 30,069,230.

Estimated Time per Respondent: .401.

Total Burden Hours: 12,058,798.

Melissa Bruce,

Executive Director, Business Management Office.

[FR Doc. 2019–19020 Filed 9–3–19; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2019–0013]

CISA Reporting Forms

AGENCY: Cybersecurity Division (CSD), Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-Day notice and request for comments; revision, 1670–0037.

SUMMARY: DHS CISA CSD will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until November 4, 2019.

ADDRESSES: You may submit comments, identified by docket number CISA–2019–0013, by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.
- *Email: fed_ir_update@hq.dhs.gov.* Please include docket number CISA–2019–0013 in the subject line of the message.
- *Mail:* Written comments and questions about this Information Collection Request should be forwarded to DHS/CISA/CSD, ATTN: 1670–0037, 245 Murray Lane SW, Mail Stop 0613, Washington, DC 20598–0613.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket and comments received, please go to *www.regulations.gov* and enter docket number CISA–2019–0013.

Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an email comment, your email address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public notwithstanding the inclusion of the routine notice.

FOR FURTHER INFORMATION CONTACT: Lisa Barr at 703.705.6078 or at *fed_ir_update@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: Section 2209 of the Homeland Security Act, as amended, established a national cybersecurity and communications integration center to function as ''a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities.'' 6 U.S.C. 659(c)(1). The Federal Information Security Modernization Act of 2014 (FISMA) establishes a federal information security incident center, and requires the Department to operate it. 44 U.S.C. 3556(a).

The Cybersecurity and Infrastructure Security Agency (CISA) operates the federal information security incident center. Through this center, FISMA requires the Department to provide technical assistance and guidance on detecting and handling security incidents, compile and analyze incident information that threatens information security, inform agencies of current and potential threats and vulnerabilities, and provide intelligence or other information about cyber threats, vulnerabilities, and incidents to agencies. 44 U.S.C. 3556(a). FISMA also requires agencies to report information security incidents, major incidents, and data breaches to the federal information security incident center. 44 U.S.C. 3556(b) (information security incidents), 44 U.S.C. 3554(b)(7)(C)(iii)(III) (major incidents); Public Law 113–283, 2(d) (2014) (codified at 44 U.S.C. 3553, note (Breaches)). The Cybersecurity Information Sharing Act of 2015 (CISA 2015) requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with certain federal entities in an automated and real-time manner. 6 U.S.C. 1504(c).

CISA is responsible for performing, coordinating, and supporting response to information security incidents, which may originate outside the Federal community and affect users within it, or originate within the Federal community and affect users outside of it. Often, therefore, the effective handling of security incidents relies on information sharing among individual users, industry, and the Federal Government, which may be facilitated by and through CISA.

Per the Federal Information Security Modernization Act of 2014, CISA operates the Federal information security incident center for the United States federal government. Each federal agency is required to notify and consult with CISA regarding information security incidents involving the information and information systems (managed by a federal agency, contractor, or other source) that support the operations and assets of the agency. Additional entities report incident information to CISA voluntarily.

CISA's website (at US–CERT.gov) is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with CISA. Constituents, which may include anyone or any entity in the public, use forms located on the website to complete these activities.

By accepting incident reports and feedback, and interacting among federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public, CISA has provided a way for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government about cybersecurity. The information is collected via the following forms:

1. The Incident Reporting Form, DHS Cyber Threat Indicator and Defensive Measure Submission System and Malware Analysis Submission Form enable end users to report incidents and indicators as well as submit malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

2. The Mail Lists Form enables end users to subscribe to the National Cyber Awareness System's mailing lists, which deliver the content of and links to CISA's information sharing products. The user must provide an email address in order to subscribe or unsubscribe, though both of these actions are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

3. The Cyber Security Evaluation Tool (CSET) Download Form, which requests the name, email address, organization, infrastructure sector, country, and intended use of those seeking to download the CSET. All requested fields are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

In order to be responsive to an ever-changing cybersecurity environment, the forms may change to collect data related to current capabilities or vulnerabilities. Standards, guidelines, and requirements of the CISA are perpetually adapting to the volatile cybersecurity environment. We must retain the ability to update these forms as required, or we will be unable to collect critical incident data in support of our mission. Without the necessary tools and methods to collect this information, we will be unable to effectively satisfy mission requirements and support our stakeholders through information collection, analysis, and exchange. The general scope and purpose of the forms will remain the same.

Incident reports are primarily submitted using CISA's Automated Indicator Sharing program. Alternately, information may be collected through web-based electronic forms, email, or telephone. Web form submission is also used as the collection method for the other forms listed. These methods enable individuals, private sector entities, personnel working at other federal or state agencies, and international entities, including individuals, companies and other nations' governments to submit information.

This is a revision to an existing form. The changes to the collection since the previous OMB approval include: Updating the name of the Agency from NPPD to CISA, updating the Incident Reporting Form, removing the ICSJWG FORM, and updating the burden and cost estimates.

The Incident Reporting Form was updated to add reporting options; and updated to improve user-friendliness by having the form be directional. The changes include: Adding structured, distinct options for reporting incidents, major incidents, breaches, and events under investigation; and adding fields to collect expanded information on topics including attack vectors, indicators of compromise, communications from compromised systems, critical infrastructure sectors, memory captures, system and network logs, and unattributed cyber intrusions.

This is a revised information collection.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submissions of responses.

Title of Collection: CISA Reporting Forms.

OMB Control Number: 1670–0037.

Frequency: Annually.

Affected Public: State, Local, Tribal, and Territorial Governments, Private Sector, and Academia.

Number of Annualized Respondents: 139,125.

Estimated Time per Respondent: 0.3333 hours, 0.1667 hours, or 0.0167 hours.

Total Annualized Burden Hours: 13,852 hours.

Total Annualized Respondent Opportunity Cost: $504,494.

Total Annualized Respondent Out-of-Pocket Cost: $0.

Total Annualized Government Cost: $2,100,032.

Scott Libby,

Deputy Chief Information Officer.

[FR Doc. 2019–19022 Filed 9–3–19; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

RIN 1601–AA91

Designation of REAL ID Identity Documents for Citizens of the Freely Associated States; Unexpired Foreign Passport With an Approved Form I–94, Documenting the Applicant's Most Recent Admission to the United States

AGENCY: Office of Strategy, Policy, and Plans, Department of Homeland Security (DHS).

ACTION: Notice designating identity documents for citizens of the Freely Associated States applying for a REAL ID driver's license or identification card.

SUMMARY: This notice announces that the Department of Homeland Security (DHS) is designating an unexpired foreign passport and valid Form I–94 (Arrival-Departure Record) as acceptable identity documentation for purposes of obtaining a REAL ID driver's license or identification card for eligible citizens of the Federated States of Micronesia, the Republic of Palau, and the Republic of the Marshall Islands (collectively known as the Freely Associated States, or FAS).

DATES: This designation takes effect September 4, 2019.

FOR FURTHER INFORMATION CONTACT: Steve Yonkers, Director, Biometrics and Credentialing/REAL ID Program, Department of Homeland Security, Washington, DC 20528, telephone (202) 282–9708; email *realid@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

A. The REAL ID Act

The REAL ID Act (the Act) was enacted in 2005 in response to a recommendation from the 9/11 Commission to improve the security of forms of identification such as state-issued driver's licenses and identification cards.[1] The Act sets minimum standards for the issuance and production of state driver's licenses and identification cards in order for federal agencies to accept those documents for official purposes, which include accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes the Secretary of Homeland Security shall determine.

B. The Compacts of Free Association

The Compacts of Free Association (COFAs) between the United States and the Freely Associated States allow most citizens of the Federated States of Micronesia (FSM), the Republic of Palau, and the Republic of the Marshall Islands (RMI) to be admitted to the United States as nonimmigrants without having to obtain a visa, and to indefinitely reside, work and study in the United States.[2]

C. REAL ID Act Modification for Freely Associated States Act

In December 2018, President Trump signed the REAL ID Act Modification for Freely Associated States Act (REAL ID Modification Act).[3] The REAL ID Modification Act authorizes states to issue full-term REAL ID-compliant driver's licenses and identification cards

[1] The REAL ID Act of 2005—title II of division B of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Public Law 109–13, 119 Stat. 231, 302 (May 11, 2005) (codified at 49 U.S.C. 30301 note).

[2] *See* Public Law 108–188 (48 U.S.C. 1921 note) (Republic of the Marshall Islands and Federated States of Micronesia); Public Law 99–658 (48 U.S.C. 1931 and 1931 note) (Palau).

[3] Public Law 115–323.