Privacy Impact Assessment

for the

Guam-Commonwealth of the Northern Mariana Islands Visa Waiver Program

DHS Reference No. DHS/CBP/PIA-079

January 18, 2024

Homeland Security

Abstract

In general, nonimmigrant visitors to the U.S. territories of Guam and the Commonwealth of the Northern Mariana Islands (CNMI) are required to obtain a visa from the U.S. Department of State before being admitted. CBP created the Guam-Commonwealth of the Northern Mariana Islands (G-CNMI) Visa Waiver Program (VWP) which allows certain nonimmigrant visitors to seek admission to Guam and/or the CNMI without a visa for a period of authorized stay not to exceed 45 days. Nonimmigrants use the Form I-736, *Guam-CNMI Visa Waiver Information*, to determine eligibility to travel under the G-CNMI Visa Waiver Program. The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is publishing this Privacy Impact Assessment (PIA) to provide notice and assess the privacy risks associated with the G-CNMI Visa Waiver Program, including the newly created restricted sub-program CNMI Economic Vitality & Security Travel Authorization Program (EVS-TAP), and the newly established electronic Form I-736, which is used to grant travel authorization to nonimmigrants prior to their embarkation to Guam or the CNMI.

Overview

In 2009, DHS/CBP issued an interim final rule (IFR)[1] in the Federal Register replacing the then-existing Guam Visa Waiver Program with the G-CNMI Visa Waiver Program. Under the previous Guam Visa Waiver Program, citizens of eligible countries or geographic areas were permitted to apply for admission to Guam at a Guam Port of Entry (POE) as nonimmigrant visitors for a period of 15 days or less, for business or pleasure, without first obtaining a nonimmigrant visa, provided that they are otherwise eligible for admission under applicable statutory and regulatory requirements.[2] The 2009 Interim Final Rule also set forth the requirements for nonimmigrant visitors seeking admission into the U.S. territories, Guam, and the CNMI.[3] Public Law 110-229 permits the Secretary of Homeland Security to create a visa waiver program for

[1] *See* 74 FR 2824 (January 16, 2009).

[2] Under the existing program, eligible participants must be a citizen of a country that: (i) has a visa refusal rate of 16.9% or less, or a country whose visa refusal rate exceeds 16.9% and has an established pre-inspection or preclearance program, pursuant to a bilateral agreement with the United States; (ii) is within geographical proximity to Guam unless the country has a substantial volume of nonimmigrant admissions to Guam as determined by the Commissioner of CBP and extends reciprocal privileges to citizens of the United States; (iii) is not designated by the Department of State as being of special humanitarian concern; and (iv) poses no threat to the welfare, safety, or security of the United States, its territories, or commonwealths (*See* https://www.ecfr.gov/current/title-8/section-212.1). The existing regulations also provide that any potential threats to the welfare, safety, or security of the United States, its territories, or commonwealths be dealt with on a country-by-country basis. A determination by the Secretary of Homeland Security that a threat existed will result in the immediate deletion of the country from the listing of eligible countries.

[3] Guam and the CNMI are considered U.S. territories. While U.S. territories fall under the jurisdiction of the U.S. federal government, they are not considered states and do not hold the same status as one (e.g., U.S. territories are not represented as part of the United States Congress).

Guam and CNMI that permits nonimmigrants from certain countries[4] to be exempt from the visa requirement when seeking entry into the United States as a visitor for a maximum stay of 45 days, provided that no potential threat exists to the welfare, safety, or security of the United States or its territories, and other criteria are met. The G-CNMI Visa Waiver Program is similar but distinctly different from the Electronic System for Travel Authorization (ESTA),[5] an application and screening system used to determine whether citizens and nationals from countries participating in the Visa Waiver Program[6] are eligible to travel to the contiguous United States.

To be eligible to travel under the G-CNMI Visa Waiver Program, prior to embarking on a carrier for travel to Guam or the CNMI, each nonimmigrant must:

- Be a national of a country or geographic area listed in 8 C.F.R. § 212.1;
- Be classifiable as a visitor for business or pleasure;
- Be solely entering and staying on Guam or the CNMI for a period not to exceed 45 days;
- Be in possession of a round trip ticket[7] that is nonrefundable and nontransferable and bears a confirmed departure date not exceeding 45 days from the date of admission to Guam or the CNMI;
- Be in possession of a completed and signed CBP Form I-736, *Guam-CNMI Visa Waiver Information*;
- Be in possession of a completed I-94, *Arrival/Departure Record*;
- Be in possession of a valid unexpired International Civil Aviation Organization (ICAO) compliant, machine-readable passport issued by a country eligible to travel to Guam or CNMI under the G-CNMI Visa Waiver Program;

[4] Travelers from the following countries may participate in the G-CNMI Visa Waiver Program: Australia, Brunei, Hong Kong, Japan, Malaysia, Nauru, New Zealand, Papua New Guinea, South Korea, Singapore, Taiwan, and the United Kingdom.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[6] Public Law 106-396 established the Visa Waiver Program, which permits citizens of designated participating countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those designated participating countries must permit U.S. citizens and nationals to travel to their countries for a similar length of time without a visa for business or tourism purposes.

[7] "Round trip ticket" includes any return trip transportation ticket issued by a participating carrier, electronic ticket record, airline employee passes indicating return passage, individual vouchers for return passage, group vouchers for return passage for charter flights, or military travel orders which include military dependents for return to duty stations outside the United States on U.S. military flights.

- Have not previously violated the terms of any prior admissions;[8]
- Acknowledge and waive any right to review or appeal an immigration officer's determination of admissibility at the port of entry into Guam or the CNMI;
- Acknowledge and waive any right to contest any action for deportation or removal, other than on the basis of an application for withholding of removal under section 241(b)(3) of the Immigration and Nationality Act (INA); withholding or deferral of removal under the regulations implementing Article 3 of the United Nations Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; or, an application for asylum if permitted under section 208 of the Act; and
- If a resident of Taiwan, possess a Taiwan National Identity Card and a valid Taiwan passport with a valid re-entry permit.

Historical Paper Process for the Form I-736

Since the inception of the G-CNMI Visa Waiver Program, CBP has required nonimmigrants to complete a paper Form I-736, *Guam-CNMI Visa Waiver Information*, in lieu of the visa requirement.[9] Nonimmigrants completed, printed, and signed the paper Form I-736 prior to their embarkation to Guam or the CNMI.[10] The paper Form I-736 requested biographic information and responses to eligibility questions that were necessary to determine the eligibility of the nonimmigrant to travel to under the G-CNMI Visa Waiver Program. The paper Form I-736 also had a set of eligibility questions that were used to determine the eligibility of the individual to travel to Guam or the CNMI and whether such travel posed a law enforcement or security risk. Upon arrival at their embarkation location, nonimmigrants were required to present the form to the carrier personnel prior to departure.[11]

[8] Prior admissions include those under the G-CNMI Visa Waiver Program, the prior Guam Visa Waiver Program, the Visa Waiver Program as described in section 217(a) of the INA, and admissions pursuant to any immigrant or nonimmigrant visa.

[9] For any of the following conditions, an I-736 is not required: (1) the traveler holds a valid visa for travel to the United States; (2) the traveler is a citizen of Australia, Brunei, Japan, New Zealand, South Korea, Singapore, Taiwan, or the United Kingdom and has a current Electronic System for Travel Authorization enrollment; or (3) a traveler from the People's Republic of China holds a valid visa for travel to the United States and has a valid Electronic Visa Update System (EVUS) enrollment.

[10] Nonimmigrants could obtain the Form I-736 through CBP's website, and then complete the form electronically, print it, and provide it to the CBP officer. Nonimmigrants also had the option to print and complete the form by hand. Additionally, nonimmigrants could receive a paper version of Form I-736 from the carrier upon their disembarkation to Guam or the CNMI.

[11] While there has historically been a requirement to present a completed and signed I-736, no penalties or fines have been issued to carriers who did not require nonimmigrants to present the signed form prior to or at the time of boarding.

Upon arrival at either the Federal Inspection Station (FIS) at a Guam or CNMI port of entry, nonimmigrants provided CBP officers with the completed paper Form I-736. The CBP officer reviewed the completed Form I-736 as part of the standard inspection process and entered information from the form into the G-CNMI database, a subsystem under the TECS security boundary.[12] The CBP officer used the information from the paper I-736 along with the information gained through the inspection to determine the nonimmigrants admissibility to Guam or the CNMI. Once the traveler was processed, the port of entry collected the paper forms and shipped them to a central storage location.

The reliance on a paper-based form and the absence of pre-arrival vetting due to the lack of automation and submission of a paper Form I-736 limited CBP's ability to implement an essential part of its national security strategy to pre-vet individuals arriving in Guam and the CNMI. Pre-vetting allows the CBP officer to have all the information from systems checks readily available as part of the officer's comprehensive admissibility determination.

As part of this strategy, CBP has implemented several advance information collections through which the agency obtains information in advance of arrival either directly from the traveler (e.g., Electronic System for Travel Authorization,[13] Trusted Traveler Programs,[14] Electronic Visa

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates) and TECS SYSTEM PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[13] The Visa Waiver Program permits eligible travelers from certain participating countries to travel to the United States without first obtaining a visa. Participation in the Visa Waiver Program requires enrollment in CBP's Electronic System for Travel Authorization program. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[14] Trusted Traveler Programs are risk-based programs that facilitate expedited processing of pre-approved low-risk travelers. CBP offers several types of Trusted Traveler Programs for arrival at air, sea, and land ports of entry. Eligible travelers who apply for a particular program are vetted against various law enforcement databases, and those who are conditionally approved are interviewed. During the interview, CBP collects biometric information. Trusted Traveler Program members are subject to recurrent vetting to ensure that these travelers do not pose threats to law enforcement or national security and to determine their continued eligibility to receive expedited processing at ports of entry. Trusted Traveler Programs are generally limited to U.S. citizens, with certain exceptions. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE GLOBAL ENROLLMENT SYSTEM (GES), DHS/CBP/PIA-002 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Update System (EVUS)[15]) or from carriers and operators (e.g., Advance Passenger Information[16] and Passenger Name Record[17]). As described above, the G-CNMI Visa Waiver Program is most like the Electronic System for Travel Authorization program, which collects information in advance to determine whether certain nonimmigrants are eligible to travel to the United States under the Visa Waiver Program. Nonimmigrants electronically submit Electronic System for Travel Authorization applications to CBP in advance for CBP to determine whether the nonimmigrant is authorized to travel to the United States. On January 18, 2024, CBP issued the Guam-Commonwealth of the Northern Mariana Islands (CNMI) Visa Waiver Program Automation and Electronic Travel Authorization; Creation of CNMI Economic Vitality & Security Travel Authorization Program (EVS-TAP) Interim Final Rule. Under this Interim Final Rule, CBP announced the automation of the Form I-736, which now requires nonimmigrants to obtain travel authorization prior to traveling to Guam or the CNMI. This interim final rule is effective September 30, 2024.

Electronic Form I-736

Like the Electronic System for Travel Authorization program, CBP is automating the submission of the Form I-736 which is available on the CBP website. Each nonimmigrant visitor wishing to travel to Guam or the CNMI under the G-CNMI Visa Waiver Program, or a representative on their behalf, must submit an electronic Form I-736 and obtain travel authorization prior to embarking on a carrier.[18] CBP recommends that G-CNMI Visa Waiver

[15] CBP's Electronic Visa Update System is a web-based enrollment system used to collect information from nonimmigrant noncitizens who 1) hold a passport that was issued by an identified country approved for inclusion in the Electronic Visa Update System program and 2) have been issued a U.S. nonimmigrant visa of a designated category. The Electronic Visa Update System, like the Electronic System for Travel Authorization program, collects updated information in advance of an individual's travel to the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC VISA UPDATE SYSTEM, DHS/CBP/PIA-033 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[16] In accordance with 19 C.F.R. §§ 122.49a, 122.49b, air carriers are required to send passenger and crew manifests to CBP before an air carrier departs from the foreign port or place for the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM, DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[17] 49 U.S.C. § 44909(c)(3) and its implementing regulation at 19 C.F.R. § 122.49d require air carriers operating flights to or from the United States to provide CBP with certain passenger reservation information, called Passenger Name Record data, to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.

[18] To accommodate people who may not have familiarity with or access to computers or the internet, DHS designed the Form I-736 website to allow a third party, such as a relative, friend, or travel agent, to submit an application on behalf of the nonimmigrant. In all cases, the nonimmigrant is responsible for the answers submitted on their behalf by a third party and the third party must check the box on the I-736 application indicating that the third party completed the application on the nonimmigrant's behalf. The email address provided should be the traveler's email address. If the nonimmigrant does not have an email address, an alternative third-party email address belonging to a point of contact (e.g., a family member, friend, or business associate) must be provided.

Program travelers obtain travel authorizations at the time of the travel reservation or purchase of the travel ticket, or at least five (5) days before departure to Guam or the CNMI to facilitate timely departures. This timeline allows for CBP to complete the necessary pre-vetting prior to an individual embarking on their travels.

As CBP transitions to an electronic Form I-736, CBP has incorporated 60day transition period into the Interim Final Rule to allow nonimmigrants to adjust to a new collection method. During this transition period, nonimmigrants and their representatives can choose to either submit the Form I-736 in advance electronically and receive electronic travel authorization prior to embarking on a carrier or submit the paper Form I-736 upon arrival. At the end of the transition period, the paper Form I-736 will become obsolete, and nonimmigrants must input and submit in advance their personal information and respond to the eligibility questions using the new electronic format.

The website offers relevant information, including who is required to submit the Form I-736, what information is needed to apply for the I-736, a link to begin the I-736 application, and how to check the status of the application. To begin the application, the nonimmigrant or representative selects the "Create New Application" option. Once selected, Security Notification,[19] Disclaimer,[20] and Privacy Act Statement pop-ups are presented to the nonimmigrant and/or representative and must be acknowledged prior to beginning the I-736.

Once all pop-us are acknowledged, the Form I-736 website prompts the individual to manually enter several pieces of information from their passport and other biographic information including:

- Full name;
- Alias;
- Date of Birth;
- City of Birth;
- Country of Birth;
- Gender;
- E-mail address;

[19] The Security Notification notifies the user that they are about to access a DHS system.
[20] The Disclaimer describes the purpose for the collection and indicates that the information provided by the individual, or on the individual's behalf by a designated third party, must be true and correct. The Disclaimer notifies the user that the information provided in the submission is used to perform checks against law enforcement databases. The Disclaimer also provides notice of administrative or criminal penalties if the individual knowingly and willfully makes a materially false, fictitious, or fraudulent statement or representation in an advance travel authorization submission.

- Phone Number, including country code;
- Home address, to include city, state/province/region, country;
- Social Media handle(s) and platform(s) used (optional);
- Destination address;
- Destination Phone number;
- Citizenship and nationality information (e.g., other country of citizenships/nationalities, how the traveler acquired citizenship/nationality, national identification number);
- Passport information (e.g., number, issuing country, issuance/expiration date);
- U.S. immigrant and nonimmigrant visa history information (e.g., place and date of application, type of visa requested, whether visa was issued/denied/withdrawn/cancelled);
- CBP Global Entry Program membership number/PASSID, if applicable;
- Parent names, if under the age of 14;
- Emergency contact information (name, email address, phone number, country);
- Responses to the following questions, such as:
    - Do you have a physical or mental disorder; or are you a drug abuser or addict; or do you currently have any of the following diseases?[21]
    - Have you ever been arrested or convicted for a crime that resulted in serious damage to property, or serious harm to another person or government authority?
    - Have you ever violated any law related to possessing, using, or distributing illegal drugs?
    - Do you seek to engage in or have you ever engaged in terrorist activities, espionage, sabotage, or genocide?
    - Have you ever committed fraud or misrepresented yourself or others to obtain, or assist others to obtain, a visa or entry into the United States?

[21] Communicable diseases are specified pursuant to section 361(b) of the Public Health Service Act: Cholera, Diphtheria, Tuberculosis infectious, Plague, Smallpox, Yellow Fever, Viral Hemorrhagic Fevers, including Ebola, Lassa, Marburg, Crimean-Congo, severe acute respiratory illnesses capable of transmission to other persons and likely to cause mortality.

- Have you ever stayed in the United States longer than the admission period granted to you by the U.S. government?
- Are you currently seeking employment in Guam or CNMI?
- Were you previously employed in the United States without prior permission from the U.S. government?
- Have you traveled to, or been present in Iraq, Syria, Iran, Sudan, Libya, Somalia, Yemen, or Cuba on or after March 1, 2011?

Once submitted, the nonimmigrant or their representative reviews the application and makes any necessary edits or corrections. CBP then uses the biographic information, including the optional social media identifiers, to conduct pre-vetting of G-CNMI bound nonimmigrants. A decision to forgo responding to the optional/voluntary social media question will not result in a denial of the travel authorization by CBP. CBP conducts vetting against selected security and law enforcement databases at DHS, including TECS[22] and the Automated Targeting System (ATS),[23] as well as publicly available sources (e.g., social media websites, even if the applicant chooses not to provide social media information). If an initial screening by CBP indicates possible information of concern, CBP may use tools and search techniques to locate and positively identify social media accounts and profiles belonging to the nonimmigrant applicant. Under no circumstance will CBP violate any social media privacy settings in the processing of the I-736 and will adhere to all Department policy regarding the use of social media information.[24] Additionally, CBP will never ask an applicant to supply their social media platform password.

Soon after the traveler inputs their information into the electronic version of Form I-736, the traveler, in most cases, will receive a positive determination of travel eligibility. The I-736 website displays the following status messages:

- **Authorization Approved** – The travel authorization has been approved and the applicant is authorized to travel to Guam and/or the CNMI under the G-CNMI Visa Waiver Program. A travel authorization does not guarantee admission into the United States as a CBP officer at a port of entry will make the final determination regarding admissibility.

---

[22] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates) and TECS SYSTEM PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e) (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[24] *See* Privacy Policy for Operational Use of Social Media Instruction 110-01-001 (2012), *available at* https://www.dhs.gov/publication/privacy-policy-operational-use-social-media-instruction-110-01-001.

- **Travel Not Authorized** – The applicant is not authorized to travel to Guam and/or the CNMI under the G-CNMI Visa Waiver Program. The applicant may be able to obtain a visa from the Department of State for travel. Please visit the Department of State website at http://www.travel.state.gov for additional information about applying for a visa. This response does not deny entry into Guam and/or the CNMI. This response only prohibits the applicant from traveling to Guam and/or the CNMI under the G-CNMI Visa Waiver Program.
- **Authorization Pending** – The applicant's travel authorization is under review because an immediate determination could not be made on the application. This response does not indicate negative findings.

If travel is not authorized, the individual is not eligible to travel to Guam or the CNMI under the G-CNMI Visa Waiver Program and will need to obtain a visa. If the application is approved, the approval establishes that the nonimmigrant is eligible to travel to Guam or the CNMI under the G-CNMI Visa Waiver Program but does not guarantee admission into Guam or the CNMI. Upon arrival to Guam or the CNMI, the nonimmigrant is subject to an inspection by a CBP officer who ultimately determines the nonimmigrant's admissibility. Under the 2024 Interim Final Rule, the CBP officer will now have access to the traveler's electronic version of Form I-736 in advance of and prior to arrival at Guam or the CNMI. Having the traveler's personal and travel information in advance will help CBP officers make a more efficient determination of admissibility. The process is also expected to help travelers by potentially shortening their time at inspection, as well as potentially decreasing the number of travelers turned away at the port of entry because of inadmissibility. Another anticipated outcome of this program is that carriers are expected to experience a decrease in costs from transporting individuals who are expected to be deemed to be inadmissible to Guam or the CNMI.

Each approved travel authorization is valid for a period of no more than 2 years.[25] A nonimmigrant with an approved Form I-736 may generally travel to Guam or the CNMI repeatedly within the validity period of the travel authorization using the same travel authorization. Nonimmigrants whose G-CNMI Visa Waiver Program electronic travel authorization applications are approved, but whose passports will expire in less than two (2) years, will receive travel authorization that is valid only until the expiration date on the passport.

[25] The Secretary of Homeland Security, in consultation with the Secretary of State, may increase or decrease the G-CNMI Visa Waiver Program travel authorization validity period for a designated G-CNMI Visa Waiver Program country or geographic area. Notice of any change to the G-CNMI Visa Waiver Program travel authorization validity periods will be published in the *Federal Register*. The G-CNMI Visa Waiver Program website will be updated to reflect the specific G-CNMI Visa Waiver Program travel authorization validity period for each G-CNMI Visa Waiver Program country or geographic area.

CNMI Economic Vitality & Security Travel Authorization Program (EVS-TAP)[26]

The 2024 Interim Final Rule created the CNMI Economic Vitality & Security Travel Authorization Program as a restricted sub-program of the G-CNMI Visa Waiver Program under the Consolidated Natural Resources Act of 2008 (CNRA) pursuant to consultations under Section 902 of the Covenant to Establish the CNMI in Political Union with the United States of America (Covenant). Citizens and nationals from the People's Republic of China (PRC) are not eligible to travel under the G-CNMI Visa Waiver Program. Rather, Chinese citizens and nationals are required to complete Form I-736 to be granted temporary admission into CNMI only without a visa. The CNMI Economic Vitality & Security Travel Authorization Program allows pre-screened nationals of the People's Republic of China to travel to the CNMI without a visa under specified conditions.

The Economic Vitality & Security Travel Authorization Program is very similar to the G-CNMI Visa Waiver Program. The primary differences are that CNMI Economic Vitality & Security Travel Authorization Program travelers may visit the CNMI only for a maximum of 14 days, whereas the G-CNMI Visa Waiver Program travelers may visit both the CNMI and Guam for a maximum of 45 days. Additionally, CNMI Economic Vitality & Security Travel Authorization Program regulations are tailored to a discrete group consisting of People's Republic of China nationals, while the G-CNMI Visa Waiver Program regulations must provide for a larger and more varied group of the countries and geographic area whose travelers are eligible for the G-CNMI Visa Waiver Program. To be considered eligible for travel authorization to the CNMI under the CNMI Economic Vitality & Security Travel Authorization Program, prior to embarking on a carrier for travel to the CNMI, nonimmigrant visitors must:

- Be a national of the People's Republic of China;
- Be classifiable as a visitor for business or pleasure;
- Be solely entering and staying on the CNMI for a period not to exceed 14 days;
- Be in possession of a round trip ticket[27] that is nonrefundable and nontransferable and bears a confirmed departure date not exceeding 14 days from the date of admission to the CNMI;
- Receive an electronic travel authorization from CBP pursuant to new paragraph 8 CFR 212.1(r)(9);

[26] CNMI EVS-TAP will be implemented 45 days after publication of a subsequent notification in the *Federal Register*.

[27] "Round trip ticket" includes any return trip transportation ticket issued by a participating carrier, electronic ticket record, airline employee passes indicating return passage, individual vouchers for return passage, group vouchers for return passage for charter flights, or military travel orders which include military dependents for return to duty stations outside the United States on U.S. military flights.

- Be in possession of a completed and signed CBP Form I-94, *Arrival-Departure Record*;
- Be in possession of a valid unexpired International Civil Aviation Organization compliant, machine-readable passport issued by the People's Republic of China;
- Have not previously violated the terms of any prior admissions or parole;
- Acknowledge and waive any right to review or appeal an immigration officer's determination of admissibility at the port of entry into the CNMI; and
- Acknowledge and waive any right to contest any action for deportation or removal, other than on the basis of: (1) an application for withholding of removal under section 241(b)(3) of the INA; (2) withholding or deferral of removal under the regulations implementing Article 3 of the United Nations Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; or, (3) after December 31, 2029, an application for asylum if permitted under section 208 of the INA. As in the G-CNMI Visa Waiver Program, section 208 of the INA regarding asylum does not apply to the CNMI during the transition period. See 48 U.S.C. § 1806(a)(7). The transition period was extended to December 31, 2029, by the Northern Mariana Islands U.S. Workforce Act of 2018, Pub. L. 115-218 (July 24, 2018).

People's Republic of China nationals who complete the Form I-736 will be prompted to complete a supplementary section of the I-736 to meet the CNMI Economic Vitality & Security Travel Authorization Program requirements. After completing the I-736 data fields, People's Republic of China nationals will be prompted to respond to the following set of questions:

- Are you traveling with someone else?
- Are any of your children born in the U.S.A.? If so, please include the place of birth.
- Are you pregnant?
- Are you coming to give birth?
- Do you have a source of income to cover for medical expenses during this trip?
- List the dates of your previous visits to the CNMI during the last year.
- How long do you intend to stay in the CNMI on this trip?
- What is your occupation?
- How long have you been employed in this occupation?

- Have you previously worked in the CNMI? If so, please include when and where.
- Have you visited the CNMI during the last 24 months?
- Do you have a residence (e.g., house, apartment, flat, condo) that you maintain control of and that you intend to return to upon the conclusion of this trip?
- Are you carrying over $10,000 on monetary instruments?
- What countries have you traveled to in the last 2 years?

Requiring a CNMI Economic Vitality & Security Travel Authorization Program electronic travel authorization will potentially reduce the number of travelers who are expected to be determined to be inadmissible to the CNMI during inspection at a port of entry, thereby saving, among other things, the cost of return travel to the carrier, inspection time, and delays and inconvenience for the traveler. Requiring a CNMI Economic Vitality & Security Travel Authorization Program electronic travel authorization also will enable the U.S. government to better allocate existing resources toward screening passengers at CNMI ports of entry, thereby facilitating legitimate travel. Requiring a CNMI Economic Vitality & Security Travel Authorization Program electronic travel authorization increases the amount of information available to CBP regarding CNMI Economic Vitality & Security Travel Authorization Program travelers before such travelers arrive at the CNMI port of entry; and, by recommending that travelers submit such information a minimum of 5 days in advance of departure, provides DHS with additional time to screen CNMI Economic Vitality & Security Travel Authorization Program travelers destined for the CNMI, thus enhancing security.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The authorities supporting CBP's collection and use of the Form I-736 data include section 702(b) of the Consolidated Natural Resources Act of 2008, Public Law 110-229, 122 Stat. 754, 860, codified at 8 U.S.C. §§ 1182(a)(7)(B), 1182(l), 1184(a)(1); 8 U.S.C. §§ 1103(a), 1357(b); and the Homeland Security Act of 2002, 6 U.S.C. §§ 101 et seq. Additionally, 8 C.F.R. 212.1 outlines the documentary requirements for nonimmigrants to enter the United States.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following System of Records Notices permit the collection and use of information for the

G-CNMI Visa Waiver Program:

- DHS/CBP-016 Nonimmigrant Information System, which serves as a repository of records for persons arriving in or departing from the United States as nonimmigrant visitors and is used for entry screening, admissibility, and benefits purposes.[28]
- DHS/CBP-009 Electronic System for Travel Authorization (ESTA), which allows for the collection, storage, and use of the information collected on the Form I-736 to determine whether applicants are eligible to travel to the United States under the Visa Waiver Program.[29]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The I-736 is stored in the G-CNMI database, which resides in the TECS security boundary. All CBP systems undergo a security authorization process (SAP) in accordance with the requirements defined under the Federal Information Security Management Act (FISMA). The most recent security authorization process for TECS was completed in December 2014 and TECS received a renewed Authority to Operate in December 2020.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CBP is working with NARA to create a records retention schedule. CBP is proposing to retain the information for 3 years in active status from the date of submission and 6 years archived, for a total of 9 years. Data linked at any time during the 9-year retention period to active law enforcement lookout records, that is matched by CBP to enforcement activities and/or investigations or cases, including travel authorizations that are denied approval to travel, will remain accessible for the life of the law enforcement activities to which they may become related.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Yes. This collection of information is subject to the Paperwork Reduction Act. The collection of information is covered by OMB Control Number is 1651-0109.

[28] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015) *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[29] *See* DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 84 FR 30746 (June 27, 2019), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The CBP Form I-736, *Guam-CNMI Visa Waiver Information*, gathers information on travelers from visa waiver countries to determine their admissibility to enter Guam or the CNMI. The Form I-736 collects the following information:

- Full name;
- Alias;
- Date of Birth;
- City of Birth;
- Country of Birth;
- Gender;
- E-mail address;
- Phone Number, including country code;
- Home address, to include city, state/province/region, country;
- Social Media handle(s) and platform(s) used (optional);
- Destination address;
- Destination Phone number;
- Citizenship and nationality information (e.g., other country of citizenships/nationalities, how the traveler acquired citizenship/nationality, national identification number);
- Passport information (e.g., number, issuing country, issuance/expiration date);
- U.S. immigrant and nonimmigrant visa history information (e.g., place and date of application, type of visa requested, whether visa was issued/denied/withdrawn/cancelled);
- CBP Global Entry Program membership number/PASSID, if applicable;
- Parent names, if under the age of 14;
- Emergency contact information (name, email address, phone number, country);
- Responses to the following questions, such as:

- Do you have a physical or mental disorder; or are you a drug abuser or addict; or do you currently have any of the communicable diseases as specified pursuant to section 361(b) of the Public Health Service Act?[30]
- Have you ever been arrested or convicted for a crime that resulted in serious damage to property, or serious harm to another person or government authority?
- Have you ever violated any law related to possessing, using, or distributing illegal drugs?
- Do you seek to engage in or have you ever engaged in terrorist activities, espionage, sabotage, or genocide?
- Have you ever committed fraud or misrepresented yourself or others to obtain, or assist others to obtain, a visa or entry into the United States?
- Have you ever stayed in the United States longer than the admission period granted to you by the U.S. government?
- Are you currently seeking employment in Guam or CNMI?
- Were you previously employed in the United States without prior permission from the U.S. government?
- Have you traveled to, or been present in Iraq, Syria, Iran, Sudan, Libya, Somalia, Yemen, or Cuba on or after March 1, 2011?

- Signature; and
- IP Address.[31]

The CNMI Economic Vitality & Security Travel Authorization Program will also add the following questions to the application:

- Are you traveling with someone else?
- Are any of your children born in the U.S.A.? If so, please include the place

[30] Communicable diseases are specified pursuant to section 361(b) of the Public Health Service Act: Cholera, Diphtheria, Tuberculosis infectious, Plague, Smallpox, Yellow Fever, Viral Hemorrhagic Fevers, including Ebola, Lassa, Marburg, Crimean-Congo, severe acute respiratory illnesses capable of transmission to other persons and likely to cause mortality

[31] The IP address provides a useful data point to identify possible fraudulent applications and/or ineligible applicants. CBP collects the IP address to assist CBP in determining which applicants are eligible to travel under the G-CNMI Visa Waiver Program. The IP address will be provided with the rest of the G-CNMI application information to the Automated Targeting System for vetting, targeting, and law enforcement purposes. CBP will use the same security and control measures to protect the IP address as it uses for the rest of the application data.

of birth.

- Are you pregnant?
- Are you coming to give birth?
- Do you have a source of income to cover for medical expenses during this trip?
- List the dates of your previous visits to the CNMI during the last year.
- How long do you intend to stay in the CNMI on this trip?
- What is your occupation?
- How long have you been employed in this occupation?
- Have you previously worked in the CNMI? If so, please include when and where.
- Have you visited the CNMI during the last 24 months?
- Do you have a residence (e.g., house, apartment, flat, condo) that you maintain control of and that you intend to return to upon the conclusion of this trip?
- Are you carrying over $10,000 on monetary instruments?
- What countries have you traveled to in the last 2 years?

2.2 What are the sources of the information and how is the information collected for the project?

Information is collected directly from an individual or representative (e.g., co-traveler, organization) who submits information on behalf of the individual. Information is submitted through the I-736 website.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. The Form I-736 and the G-CNMI database do not collect, use, maintain, or disseminate information from commercial sources or publicly available information. However, CBP collects optional social media information from nonimmigrants seeking to travel under the G-CNMI Visa Waiver Program. Should an individual choose to provide their social media identifier(s), and an initial screening by CBP indicates possible information of concern, CBP may use tools and search techniques to locate and positively identify social media accounts and profiles belonging to the

applicant. CBP reviews social media in addition to the DHS system checks described above to further assess an individual's eligibility to travel to Guam or the CNMI, irrespective of whether an individual voluntarily provides social media information as part of their application.

2.4 Discuss how accuracy of the data is ensured.

CBP collects this information directly from the nonimmigrant and/or representative on behalf of the nonimmigrant applying for travel authorization. While there is always an inherent risk to manual data entry, the nonimmigrant and/or representative can review and verify the information prior to submission to CBP. If a nonimmigrant submitted incorrect information on the I-736, they have the option to update the information. Nonimmigrants can visit the I-736 website and select the Review/Update I-736 option. Once the option is selected, the nonimmigrants are directed to enter a combination of either their Form I-736 Reference number/Passport number or Passport/Name/Date of Birth. By inputting this information, the tool retrieves the previously submitted information and allows for the individual to correct or update the existing information. Moreover, during the inspection process, a CBP officer will verify and update any information that is incorrect or inaccurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of inappropriate collection of First Amendment protected information, as regulated by the Privacy Act, 5 U.S.C. § 552a(e)(7).

Mitigation: This risk is partially mitigated. The application will specify that the social media field is optional. However, irrespective of whether the individual optionally provides their social media information, First Amendment-protected information could be collected when CBP officers use publicly available information, including social media information, as part of the existing CBP screening and vetting processes pursuant to DHS and CBP's law enforcement mission authorities. While there is a risk of collection of First Amendment-protected activity by CBP, collection that is pertinent to, and within the scope of, an authorized CBP law enforcement activity is permitted under the Privacy Act. DHS policy directs that "DHS personnel shall not collect, maintain in DHS systems, or use information protected by the First Amendment unless (a) an individual has expressly granted their consent for DHS to collect, maintain and use that information; (b) maintaining the record is expressly authorized by a federal statute; or (c) that information is relevant to a criminal, civil, or administrative activity relating to a law DHS enforces or administers." In addition, there remains the possibility that some other information within the scope of subsection (e)(7)—either content shared by the applicant following admission into the United States territory or content from others, such as U.S. citizens, appearing within the applicant's social media profile—may be collected during the vetting process. While the information may be used to approve or deny a G-CNMI Visa Waiver Program application, CBP

will not collect, maintain, and/or use such third-party information unless it is necessary and relevant to making a G-CNMI Visa Waiver Program determination. Further, any such collection must be within the scope of an authorized law enforcement activity, as permitted by subsection (e)(7).

Privacy Risk: There is a risk CBP may make G-CNMI Visa Waiver Program determinations based on inaccurate information posted on social media.

Mitigation: This risk is partially mitigated. Information is collected directly from the social media accounts of individuals who are presumed to generally have some degree of control over what is posted on their social media account. CBP, therefore, presumes some of this information is accurate. However, information posted by an associate of the individual on the individual's social media page may also be taken into consideration. Information collected from social media, by itself, will not serve as the sole basis to deny an application. Instead, CBP uses the totality of information – information submitted as part of the G-CNMI Visa Waiver Program application along with the information found during CBP vetting, including on social media – to approve or deny the application. CBP has also developed procedures and training focused on understanding data quality limitations associated with social media.

Privacy Risk: There is a risk that CBP may collect information about other individuals who may have posted or interacted with the G-CNMI Visa Waiver Program applicant on their social media platform(s) yet are not G-CNMI Visa Waiver Program applicants themselves and have no other involvement with DHS or CBP.

Mitigation: This risk is partially mitigated. As described above, CBP will view information about individuals who are associated with an applicant's social media account, and possibly individuals associated with those individuals, even if the individuals do not have a direct connection with CBP. However, CBP will not retain such information unless it is relevant to a determination on a G-CNMI Visa Waiver Program application.

Privacy Risk: There is a risk of overcollection since CBP may collect information about individuals who do not travel to Guam or the CNMI.

Mitigation: This risk is partially mitigated. CBP is collecting this information from or about nonimmigrants who are seeking to travel to Guam or the CNMI. These individuals are required to obtain travel authorization prior to traveling to Guam or the CNMI. It is possible for a nonimmigrant to obtain travel authorization and ultimately not travel to Guam or the CNMI. This circumstance is like other advance information collections, such as Advance Passenger Information (API) data,[32] where a commercial travel carrier submits certain advance information

[32] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM, DHS/CBP/PIA-001 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-

on passengers intending to travel to the United States. With Advance Passenger Information, CBP may also collect and retain information on individuals who may intend to travel but fail to board the carrier. However, this information, combined with the results of the pre-vetting, is necessary and is used by CBP to identify public safety threats (such as wants/warrants) and national security threats (such as links to terrorist organizations).

Privacy Risk: There is a risk that CBP is collecting more information than necessary to grant travel authorization for the G-CNMI Visa Waiver Program.

Mitigation: This risk is partially mitigated. CBP is collecting similar information from travelers to Guam and CNMI that it typically collects prior to an individual traveling to the United States (e.g., Advance Passenger Information System, Passenger Name Record data,[33] Electronic System for Travel Authorization,[34] Form I-94 *Arrival/Departure Record*[35]). Additionally, the information collected in advance of an individual's arrival is consistent with the information that CBP normally collects at the port of entry during inspection in accordance with existing CBP processes. The advance collection of this data streamlines the processing of these individuals upon their arrival to the port of entry because it enables CBP to conduct vetting prior to an individual's arrival to identify any public safety or national security concerns.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP collects information via Form I-736 to grant travel authorization to a nonimmigrant traveling to Guam and/or the CNMI without a visa. Data from the I-736 is screened and vetted against TECS, the Automated Targeting System, and other publicly available information including social media accounts. The information from the I-736 system is also used by other CBP systems to track the period of admissibility of nonimmigrants and maintain a central repository of contact information for these individuals and their emergency contacts, which may include U.S. persons. These systems transmit information to other systems to identify travel patterns, arrivals

customs-and-border-protection.

[33] U.S. law requires air carriers operating flights to, from, or through the United States to provide CBP with certain passenger reservation information, called Passenger Name Record data. The collection of Passenger Name Record data allows CBP to prevent, detect, investigate, and prosecute terrorist offenses and related crimes and certain other crimes that are transnational in nature. Air carriers are required to provide this information on all persons traveling on flights to, from, or through the United States to CBP beginning 72 hours prior to departure of a flight, and up to 24 hours before the scheduled flight departure.

[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE I-94 WEBSITE APPLICATION, DHS/CBP/PIA-016 (2013 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

without departure, and nonimmigrant noncitizens overstaying their admissible terms in the United States.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. G-CNMI Visa Waiver Program data is screened and vetted against the Automated Targeting System, which compares existing information about travelers and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.

3.3 Are there other components with assigned roles and responsibilities within the system?

The G-CNMI Visa Waiver Program information is stored in a segmented database in TECS and is typically not available for access by other DHS components. However, if CBP creates an Automated Targeting System Unified Passenger (UPAX) event based on pre-arrival vetting, the Unified Passenger event will be accessible by DHS components that have access to the Targeting Framework within the Automated Targeting System. Furthermore, secondary inspections that result in adverse or administrative immigration actions are automatically sent to U.S. Immigration and Customs Enforcement (ICE) and stored in the Enforcement Integrated Database (EID)[36] as immigration events.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that CBP will inappropriately access information that is not publicly available.

Mitigation: This risk is partially mitigated. CBP analysts are required to respect an individual's privacy settings on social media accounts. CBP analysts will review information on social media platforms in a manner consistent with the privacy settings the social media account holder has chosen to adopt for those platforms. Only that information which the account holder has allowed to be shared publicly will be viewed by CBP. All authorized CBP social media users must sign rules of behavior that explicitly prohibit them from accessing information designated as private on an account. Authorized users must also complete privacy training for the operational

[36] *See* U.S. DEPARTMENT OF HOMELAND SECUIRTY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015, *available at* https://www.dhs.gov/privacy-documents-ice.

use of social media. To maintain access as an operational user of social media, CBP users must complete the privacy training and attest to the rules of behavior on an annual basis. Additionally, CBP routinely reviews social media access and removes access from users who no longer require access to social media (e.g., change of job duties or employment). Furthermore, all G-CNMI Visa Waiver Program application determinations are reviewed by a first line supervisor to verify that the findings are based on all available information (not solely based on information obtained from social media) and assess the completeness and accuracy of the records used to support the determinations. Social media reviews that yield information that could result in the denial of a G-CNMI Visa Waiver Program application are reviewed by a second line supervisor to ensure that information used in the G-CNMI Visa Waiver Program determination is accurate, relevant, timely, and complete.

Privacy Risk: There is a risk that CBP will conduct pre-arrival vetting checks on individuals who do not arrive in Guam or the CNMI.

Mitigation: This risk is partially mitigated. CBP will conduct pre-arrival vetting on nonimmigrants who apply for travel authorization but do not ultimately travel to Guam or the CNMI. The purpose of the collection is to determine whether an individual is eligible to travel to Guam or the CNMI. If CBP grants a travel authorization, the individual is responsible for booking a travel reservation and ultimately boarding the plane. As described above, this collection and use is consistent with current CBP operations, such as when CBP receives Advance Passenger Information from carriers that submit information regarding travelers intending to travel to the United States but who do not arrive. In both circumstances, CBP collects information on and vets travelers to identify public safety threats (such as wants/warrants) and national security threats (such as links to terrorist organizations).

Privacy Risk: There is a risk that CBP will deny the application if, through vetting, CBP discovers a social media profile that was not disclosed on the application.

Mitigation: This risk is mitigated. As noted previously, provision of an individual's social media information is optional. Therefore, while CBP may still vet an individual using information obtained via social media, an individual's application may not be denied solely because CBP later discovered a social media profile for that individual. However, CBP may use relevant information collected from a social media account to adjudicate a travel authorization. Further, CBP advises applicants and representatives to complete the application fully and honestly; failure to provide accurate and truthful responses to required fields on the I-736 may result in denial. CBP uses discretion when reviewing applications for approval or denial in accordance with the INA.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the

collection of information? If notice is not provided, explain why not.

The Form I-736 website contains a Privacy Act Statement which includes CBP's authority to collect the information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to CBP. CBP provides general notice about the G-CNMI Visa Waiver Program through the publication of this Privacy Impact Assessment and the associated System of Records Notices identified in Section 1.2 above. Additional information, including Frequently Asked Questions (FAQ), about the G-CNMI Visa Waiver Program is available at https://i736.cbp.dhs.gov/I736/#/apply-I736 and the CBP Information Center website.[37]

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Nonimmigrants traveling to Guam or CNMI from certain countries are required to complete an electronic I-736 form prior to traveling. These individuals must receive a positive determination of travel authorization from CBP to board a plane to Guam or the CNMI. Due to this requirement, the only legitimate means of declining to provide the information is to choose not to travel Guam or the CNMI. Furthermore, nonimmigrants do not have the right to consent to uses of the information. Once an individual submits the data, they cannot exert control over the use of that data, aside from their ability to amend specific data elements by accessing their account and submitting amended data elements.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that they are required to submit a I-736 to receive travel authorization prior to travel.

Mitigation: This risk is mitigated. The individual is provided with multiple forms of notice about the I-736 requirement. DHS provided notice about the requirement through the 2024 Interim Final Rule, as well as the I-736 website. Carriers also provide notice of this requirement to individuals traveling from the designated countries to Guam or the CNMI upon booking.

Privacy Risk: There is a risk that emergency points of contact, including U.S. persons, may not be aware that their information may be recorded in the G-CNMI Visa Waiver Program application and may be used for vetting an applicant. Furthermore, these individuals will not have an opportunity to have their information removed from evaluation and/or disassociated with the G-CNMI Visa Waiver Program application.

[37] The CBP Information Center website provides easily accessible information and services via Frequently Asked Questions and links, *available at* https://help.cbp.gov/s/?language=en_US.

Mitigation: This risk is not mitigated. There is no opportunity to notify individuals, who may be named in a G-CNMI Visa Waiver Program application by the applicant or to provide an opportunity for those individuals to have their information removed from evaluation and/or disassociated with the application. To partially mitigate this risk, DHS is providing notice to the public of this new information collection by publication of the Privacy Impact Assessment to provide as much transparency into its operations as possible. If an individual believes that DHS may have information about them as part of the expanded G-CNMI Visa Waiver Program application, they are encouraged to follow the individual access, redress, and correction procedures described below.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

CBP is working with the National Archives and Records Administration to create a records retention schedule. CBP is proposing to retain the information for three (3) years in active status from the date of submission and six (6) years archived, for a total of nine (9) years. Data linked at any time during the 9-year retention period to active law enforcement lookout records and matched by CBP to enforcement activities and/or investigations or cases, including travel authorizations that are denied approval to travel, will remain accessible for the life of the law enforcement activities to which they may become related.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CBP may retain information longer than is necessary to perform relevant immigration functions.

Mitigation: This risk is not mitigated. Although there is always an inherent risk with retaining data for any length of time, data retention periods for the associated systems are consistent with the concept of retaining data to maintain a complete and accurate history of a traveler's encounter history and admissibility to enter the United States. However, because the retention schedule has not been formally completed/approved, this risk remains unmitigated. This Privacy Impact Assessment will be updated if the approved retention schedule differs from what is proposed above.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information may be shared with appropriate federal, state, local, tribal, and foreign government agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, or when DHS believes the information would assist enforcement of civil or criminal laws.

This information may be shared when CBP reasonably believes such use is to assist in anti-terrorism efforts or intelligence gathering related to national or international security or transnational crime. CBP may share information with federal and foreign government intelligence or counterterrorism agencies, or components thereof, in bulk, to assist in counterterrorism or counter-intelligence activities, consistent with an information sharing and access agreement for ongoing, systematic sharing. CBP may also share this information with federal and foreign government intelligence or counterterrorism agencies, or components thereof, in response to queries predicated on a particularized threat to national or international security, or to assist in other intelligence activities.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS will share G-CNMI Visa Waiver Program information with external organizations consistent with the routine uses in the above System of Records Notices, which are compatible with the original purpose of collection, "to collect and maintain a record of nonimmigrant aliens holding a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category, and to determine whether there is information that requires separate, additional action." CBP will memorialize these data sharing practices in Memoranda of Understanding (MOUs) or Interconnection Security Agreements (ISAs), which govern the sharing of G-CNMI Visa Waiver Program information. Under the terms of these agreements, the Department of State, other agencies, and the carriers will secure G-CNMI Visa Waiver Program information consistent with approved security practices that meet DHS standards. Personal information will be kept secure and confidential and will not be divulged to any person within or outside the G-CNMI Visa Waiver Program without an official need to know. Sharing with the Department of State is authorized for purposes of granting or revoking a visa. Recipients from other agencies and carriers will be required by the terms of the information sharing agreement to employ security features to safeguard the shared information.

6.3 Does the project place limitations on re-dissemination?

Yes. Information that is shared with other agencies, federal, state, local, tribal, or foreign governments, outside of the context of any Memorandum of Understanding or other prior written arrangement requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office

and will only be granted when the request and use are: 1) consistent with the Privacy Act and DHS policies, 2) consistent with published routine uses, and 3) with the express written approval of the CBP Privacy and Diversity Office. All three requirements are stated conditions for the receiving agencies to obtain and use the shared information. These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Memoranda of Understanding and other written arrangements defining roles and responsibilities will be executed between CBP and each agency that regularly accesses CBP information. These agreements establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy safeguards for the data.

The information may be transmitted either electronically or as printed materials to authorized personnel. Electronic communication with other, non-CBP systems, may be enabled via message/query-based protocols delivered and received over secure point-to-point network connections between CBP and non-CBP systems. CBP's external sharing complies with statutory requirements for national security and law enforcement systems.

Information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any Memoranda of Understanding/Agreement or other prior written arrangement generally requires a written request by the agency specifically identifying the type of information sought, purpose for which the information will be used, and how the information will be safeguarded. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office and documented in DHS Form 191.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be unnecessarily shared with entities outside of CBP.

Mitigation: This risk is partially mitigated. All external sharing is consistent with the Routine Uses within the published System of Records Notices or with other disclosure provisions of the Privacy Act. When information is regularly shared there is both a written Memorandum of Understanding and Interconnection Security Agreement that is negotiated between CBP and the external requestor. The written arrangements and Interconnection Security Agreements are periodically audited and reviewed by the program office in coordination with the CBP Privacy and Diversity Office and CBP's Office of Chief Counsel, and the external requestor's conformance to the use, security, and privacy considerations are verified before Certificates to Operate are issued or renewed.

When sharing information with third parties, the same requirements related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. This criterion is determined and approved during the information sharing disclosure review process by the CBP Privacy and Diversity Office. Third parties must agree to uphold the same security and privacy safeguards that are used by CBP and DHS.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

To gain access to the contact information stored by CBP, a traveler may request information about their records through procedures provided by the Freedom of Information Act (FOIA) and the access provisions of the Privacy Act of 1974 as described in DHS regulations, Part 5, Title 6 of the Code of Federal Regulations. Individuals are encouraged to make a FOIA request electronically; information about how to submit a FOIA request can be found here: https://www.dhs.gov/foia-contact-information.

When seeking records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. A traveler must provide their full name, current address, and date and place of birth. They must also provide:

- An explanation of why the individual believes DHS would have information on them;
- Details outlining when they believe the records would have been created; and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying their agreement for access to their records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP 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. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

Persons who have experienced difficulties while traveling may submit a redress request through DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for

persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

DHS Traveler Redress Inquiry Program (TRIP)
6595 Springfield Center Drive, TSA-910
Springfield, VA 22150-6901

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Travelers who wish to correct or update a previously submitted I-736, may resubmit the I-736 by visiting https://i736.cbp.dhs.gov/I736/#/home. Upon selecting the Review/Update I-736 option, nonimmigrants are directed to enter a combination of either their Reference number/Passport number or Passport/Name/Date of Birth. By inputting this information, the tool retrieves the previously submitted information and allows the traveler to correct or update the existing information. Nonimmigrants wishing to correct inaccurate information may also submit a Privacy Act Amendment request through the same access processes explained in Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

The I-736 website clearly notifies the traveler of the option to either submit a new I-736 or correct an existing one. This Privacy Impact Assessment and the I-736 website provide travelers instructions to correct any inaccurate data. If an individual experiences a delay or issue as an outcome of the processes described in this Privacy Impact Assessment, travelers are informed of the avenues for redress in Section 7.2. Signage and tear sheets at ports of entry provide information about how to contact the CBP Information Center and/or DHS TRIP. In addition, travelers may request information from the on-site CBP officer.

The CBP Information Center website provides easily accessible information and services via Frequently Asked Questions, links, and a portal where individuals or their representatives can submit a complaint or comment concerning their interactions with CBP. Executive Order 12862, *Setting Customer Service Standards,* requires all Executive departments and agencies to meet customer service standards by providing easily accessible information, services, and complaint systems, and by providing a means to address customer complaints. The CBP Information Center serves as a means for travelers to submit complaints. CBP developed the CBP Complaint Management System (CMS)[38] for travelers or their representatives to submit a complaint or

[38] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION,

comment concerning their interactions with CBP. The CBP Complaint Management System enables CBP to address customer complaints and comments by providing a unified tracking system to follow the life cycle of complaints and comments and analytical tools to measure responsiveness and customer feedback trends.

Travelers may also contact the DHS Traveler Redress Inquiry Program (DHS TRIP), 6595 Springfield Center Drive TSA-910, Springfield, VA 22150-6901 or online at www.dhs.gov/dhs-trip if they have experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate biometric information retained in their record(s). Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and the relevant System of Records Notices describe how individuals can make access requests under FOIA or the Privacy Act. CBP and DHS provide notice to the public of their redress rights on their websites. In addition, CBP officers, and tear sheets if requested, direct travelers to the CBP Info Center and DHS TRIP to learn about additional opportunities for redress. Redress is available for U.S. citizens and lawful permanent residents through requests made under the Privacy Act as described above. U.S. law does not extend Privacy Act protections to individuals who are not U.S. citizens, lawful permanent residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access or correction of records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records collected and retained pursuant to the entry process, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

PRIVACY IMPACT ASSESSMENT FOR THE COMPLIMENTS, QUESTIONS, COMPLAINTS AND COMMENTS MANAGEMENT SYSTEM (CQC2MS), DHS/CBP/PIA-035 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this Privacy Impact Assessment?

CBP implements role-based access for all CBP systems, and only grants access to users who have a demonstrated need to know. All CBP systems secure data by complying with the requirements of DHS information technology security policy, particularly the DHS Sensitive Systems Policy Directive 4300A.[39] This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. CBP periodically evaluates these systems to ensure that each complies with these security requirements. Each system provides audit trail capabilities to monitor, log, and analyze system transactions as well as actions and system accesses of authorized users. CBP periodically conducts reviews for compliance within the program and between external partners to ensure that the information is used in accordance with the stated acceptable uses documented in any applicable Memoranda of Understanding/Agreement, System of Records Notices, sharing agreements, and other technical and business documentation.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

CBP does not grant access to users of CBP systems without completion of the CBP Security and Privacy Awareness course. This training presents Privacy Act responsibilities and agency policy regarding the security, sharing, and safeguarding of both official information and personally identifiable information. The training also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and CBP system users are required to take the course annually.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

System access is based on a demonstrated need to know by a user, and access is only granted with supervisory approval and upon completion of the required security checks.

8.4 How does the project review and approve information sharing

[39] *See* DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any information sharing agreements for this data will define the nature of access, the scope of information subject to the sharing agreement, and the privacy, security, safeguarding, and other requirements. All information sharing arrangements are reviewed by the CBP Privacy Officer and the CBP Office of Chief Counsel in accordance with existing CBP and DHS policy.

Contact Official

Matthew Davies
Executive Director
Admissibility and Passenger Programs
Office of Field Operations
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
privacy.cbp@cbp.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717