Privacy Impact Assessment
for the

National Vetting Center (NVC)

DHS/ALL/PIA-072

December 11, 2018
(updated April 11, 2023)

Contact Point
Monte Hawkins
Director
National Vetting Center

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

Through National Security Presidential Memorandum (NSPM)-9, the President has mandated the Federal Government improve the manner in which executive departments and agencies (agencies) coordinate and use intelligence and other information to identify individuals who present a threat to national security, border security, homeland security, or public safety in accordance with their existing legal authorities and all applicable policy protections. To achieve this mandate, the President directed the establishment of the National Vetting Center (NVC) within the Department of Homeland Security (DHS), with the purpose of coordinating agency vetting efforts to locate and use relevant intelligence and law enforcement information to identify individuals who may present a threat to the homeland. The Secretary of Homeland Security has delegated this responsibility within DHS to U.S. Customs and Border Protection (CBP). DHS is conducting this Privacy Impact Assessment (PIA) to assess the risks to privacy, civil rights, and civil liberties presented by the NVC and the vetting programs that will operate using the NVC.

Updated Note (April 11, 2023): As previously detailed, Vetting Support Agencies electronically transmit relevant and appropriate information (Vetting Support Responses) to Adjudicating Agencies using the NVC technology. The Vetting Support Responses include links or pointers to information that Vetting Support Agencies assess are valid and analytically significant identity matches. These links or pointers allow Analysts to view related information in other (typically classified) systems to which the Analyst has authorized access. Originally, the Vetting Support Responses only included these links or pointers, which meant that Analysts had to search other systems to access additional information. Now, as an update to this Privacy Impact Assessment the Vetting Support Agencies may also provide relevant information from the Vetting Support Request that matches information in Vetting Support Agency holdings. Unlike the links or pointers information, this matched information is presented for Analysts to view in the NVC technology; however, Analysts will still need to access other systems outside of the NVC technology to view all relevant information from Vetting Support Agency holdings.

Additionally, DHS is providing notice about a privacy-related risk in the vetting process regarding the potential for an individual to change legal status during the vetting process. Additionally, the Authority to Operate for the NVC technology was modified and approved in February 2022. There are no other updates to this Privacy Impact Assessment. The descriptions of the Fair Information Practice Principles (FIPPs), risks, and mitigations remain the same as first published on December 11, 2018.

Overview

NSPM-9[1] directed the establishment of the NVC as part of the National Vetting Enterprise.[2]

[1] *See* https://www.whitehouse.gov/presidential-actionas/presidential-memorandum-optimizing-use-federal-government-information-support-national-vetting-enterprise/.
[2] NSPM-9 describes the National Vetting Enterprise as the coordinated efforts of agencies across the U.S. Government to collect, store, process, share, disseminate, and use accurate and timely biographic, biometric, and

As outlined in NSPM-9, border and immigration security are essential to ensuring the safety, security, and prosperity of the United States. Every day, the U.S. Government determines whether to permit individuals to travel to and enter the United States, ship goods across its borders, grant immigration benefits, and consider other actions that affect U.S. national and homeland security, public safety, and commerce. These decisions are made on the basis of relevant and appropriate information held across the U.S. Government, including information held by law enforcement and the Intelligence Community (IC) based upon their unique authorities and missions.

The U.S. Government has developed several different processes and procedures to evaluate an individual's suitability for access to the United States or other travel- or immigration-related benefits against information available to the U.S. Government (generally referred to as "vetting").[3] However, these current processes are often designed for single uses that only leverage portions of potentially relevant data. These processes rely heavily on primarily manual procedures that use separate technical interfaces and are not scalable or adaptable to meet ever-evolving threats. To improve security for the homeland, agencies need a consolidated process that allows for a coordinated review of relevant intelligence and law enforcement information to ensure that immigration and border security decisions are fully informed and accurately implemented by adjudicators consistent with existing authorities. Creating, maintaining, and facilitating the operation of that process is the primary mission of the NVC.

The NVC will not replace all vetting activities that occur today. Most immigration and border security programs already use readily available, unclassified information. However, the vetting processes that support those programs may face challenges when using classified or otherwise highly restricted information to support those processes.[4] The NVC process and technology is designed to make such information accessible in a more centralized and efficient manner to agencies charged with making adjudications. The NVC does not engage in making adjudications itself. Its role is limited to that of facilitator or service provider for the NVC process and technology used for vetting.

NVC activities will be conducted in a manner that is consistent with the Constitution; applicable statutes including the Privacy Act; applicable executive orders and Presidential Directives including Executive Order 12333, *United States Intelligence Activities*, as amended; and other applicable law, policies, and procedures pertaining to the appropriate handling of information

contextual information, including on a recurrent basis, so as to identify activities and associations with known or suspected threat actors and other relevant indicators that inform adjudications and determinations related to national security, border security, homeland security, or public safety.

[3] For purposes of this PIA, "vetting" is defined as manual and automated processes used to identify and analyze information in U.S. Government holdings to determine whether an individual poses a threat to national security, border security, homeland security, or public safety, primarily, but not necessarily exclusively, in support of the U.S. Government's visa, naturalization, immigration benefit, immigration enforcement, travel, and border security decisions about an individual.

[4] Highly restricted information includes information that, although not classified, is very sensitive and may require a manual review by the agency that holds that information to decide if it can be shared with another agency. This information is typically subject to legal and policy restrictions on sharing. Information about an individual who is the subject of an open criminal investigation, but is unaware of that fact, is an example of highly restricted information.

about U.S. persons (as defined in Executive Order 12333) and other individuals protected by U.S. law and policy. The NVC has not changed or expanded these existing authorities.

Scope of NVC Activities and Vetting Programs

NSPM-9 requires that the NVC "coordinate agency vetting efforts to identify individuals who present a threat to national security, border security, homeland security, or public safety." Agencies are permitted to "conduct any authorized border or immigration vetting activities through or with" the NVC. Vetting under NSPM-9 is primarily focused on "adjudications and other determinations made in support of immigration and border security," including "individuals who (i) seek a visa waiver, or other immigration benefit, or a protected status; (ii) attempt to enter the United States; or (iii) are subject to an immigration removal proceeding." This PIA uses the phrase "immigration and border security" to collectively describe the scope of these programs, vetting activities, and decisions.

The National Vetting Governance Board (Board),[5] an interagency governing body established by NSPM-9 to oversee the National Vetting Enterprise and the activities of the NVC, must approve the NVC's support for any new vetting activities. It does so with advice and support from a Legal Working Group and separate Privacy, Civil Rights, and Civil Liberties (PCRCL) Working Group,[6] both interagency groups established under NSPM-9 and charged with advising the Board and reviewing NVC plans and activities. Both Working Groups support the Board in its oversight role by informing it of the legal, privacy, civil rights, and civil liberties ramifications of any new vetting activities proposed by the NVC and recommending alternatives or modifications to such proposals that better ensure compliance with law and policy and the protection of individual privacy, civil rights, and civil liberties, as appropriate.

NSPM-9 also requires that "accurate and timely biographic, biometric, and contextual information" be used as part of the vetting process and that "activities, associations with known or suspected threat actors, and other relevant indicators" be identified and considered in making such decisions. In addition to terrorism-related threats, programs that use the NVC process and technology to facilitate vetting may also identify additional categories of threats relevant to their vetting such as transnational organized crime, foreign intelligence activities directed against the United States, the proliferation of weapons of mass destruction, malign cyber activities, and the efforts of military threat actors.[7]

As vetting programs are integrated into the NVC process and technology, this PIA will be

[5] The National Vetting Governance Board Charter can be found here: https://foiarr.cbp.gov/docs/Significant_Records_of_Interest/2018/298603947_2582/1811011114_National_Vetting_Governance_Board_Charter_(PUBLIC).pdf.
[6] The PCRCL Working Group Charter can be found here: https://foiarr.cbp.gov/docs/Significant_Records_of_Interest/2018/298603947_2583/1811011116_NVC_PCRCL_WG_Charter_(Approved_09_27_2018).pdf.
[7] *See* NSPM-7, *Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans.*

updated with an addendum that describes each such vetting program.[8]

NVC Vetting Process

The NVC process generally operates as follows.[9] U.S. Government agencies responsible for making immigration and border security decisions (Adjudicating Agencies) assign their own employees to serve as Adjudicating Agency Vetting Analysts (Vetting Analysts) who, using NVC technology, review intelligence and information potentially relevant to a particular adjudication (*e.g.*, an application for a visa waiver or a visa). This intelligence, law enforcement, and other information is made available by Vetting Support Agencies, which are the agencies that provide support to the immigration or border security program in question. After comparisons are conducted to identify information potentially relevant to a particular immigration or border security matter, the Vetting Support Agency determines if such information may be shared with the Adjudicating Agency under applicable legal standards and guidelines that govern its dissemination.

Vetting Support Agencies electronically transmit that relevant and appropriate information (Vetting Support Responses) to Adjudicating Agencies using the NVC technology. These Vetting Support Responses may include relevant information from the Vetting Support Request that matches information in Vetting Support Agency holdings as well as links or pointers to information that the Vetting Support Agencies believe are valid and analytically significant identity matches.[10] The Vetting Support Response must be cleared for dissemination by the Vetting Support Agency consistent with that Vetting Support Agency's policies, practices, and procedures, including, when applicable, the agency's guidelines concerning the collection, retention, and dissemination of U.S. person information approved by the Attorney General pursuant to Executive Order 12333 (Attorney General Guidelines).

Using NVC technology, the Vetting Support Responses are displayed to the Vetting Analyst, and the Analyst uses the links or pointers provided to view the information resident in other (typically classified) systems to which the analyst has authorized access.[11]

The Vetting Analyst then analyzes this information and considers it in relation to the relevant legal standard for deciding the matter at issue (*e.g.*, standard for issuing a visa waiver or visa) before

---

[8] Depending on the vetting program, the addendum may be classified or otherwise not publicly releasable. The Principles of Intelligence Transparency will help guide IC decisions on making information publicly available.

[9] Specific aspects of the process may vary from one vetting program to the next; however, in all instances, automated responses are reviewed manually before being considered as part of an adjudication and adjudications are performed by Adjudicating Agencies.

[10] Information that has been deemed "analytically significant" by an intelligence element is information that provides analytic insight into the potential threat to national security posed by an individual, either directly or indirectly. For Vetting Support Agencies that are elements of the IC, any U.S. person information must satisfy the requirements for dissemination under that agency's Attorney General Guidelines pursuant to Executive Order 12333 to qualify as analytically significant threat information. Such information will also be presumed to be in adherence to the IC Analytic Standards established in Intelligence Community Directive 203, *available at*https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.. The above does not apply to law enforcement information that is not foreign intelligence.

[11] Vetting Analysts may not have access to all records in a system. If the link in question is to a record to which they do not have access, Vetting Analysts will notify their supervisor to either request access or transfer the matter to another Vetting Analyst who has the appropriate level of access to view the record in question.

making a decision. The Vetting Analyst then makes a recommendation (*e.g.*, to grant or deny) to an Adjudicator, who is an official within the Adjudicating Agency that has the responsibility to make the decision. Adjudicators (who are not assigned to the NVC but sit at their home agencies) consider the Vetting Analyst's recommendation and analysis underlying that recommendation, when appropriate, along with other relevant information available to them outside of the NVC process, and make a decision (*e.g.*, approve or deny the visa waiver or visa).[12] Throughout this process, the Vetting Analysts and the Adjudicators both remain under the operational control and act under the legal authorities of the Adjudicating Agency.

Supporting the NVC process is the IC Support Element, which is also established pursuant to NSPM-9. The function of the IC Support Element is to "facilitate, guide, and coordinate all IC efforts to use classified intelligence and other relevant information within IC holdings in direct support of the NVC." It is an independent entity established by the Director of National Intelligence comprising certain IC elements, which provide support to the NVC in accordance with their existing authorities. The role of each IC element, including whether it provides information in support of a particular immigration or border security program, will vary based on the particular vetting program and each agency's individual authorities, policies, and procedures.

The composition of the IC Support Element will be a combination of assignees physically co-located at the NVC and virtual support by personnel located at the relevant IC elements' own facilities. The IC Support Element assigns on-site personnel to the NVC to support the Vetting Analysts by reaching back efficiently to the Vetting Support Agencies they represent for support, as needed. They ensure the Vetting Support Responses provided by Vetting Support Agencies are returned consistently and meet the needs of the Adjudicating Agencies.

All activities undertaken using the NVC process and technology or occurring at other agencies in support of the NVC are conducted under the existing legal authorities of the participating agencies. The NVC itself does not make operational recommendations or decisions. That authority remains with the Adjudicating Agencies under existing legal and policy frameworks.

NVC Technology and Data Management[13]

The NVC process and technology are offered as a common service to Adjudicating Agencies. Using cloud-based services and technology, the NVC technology performs the following functions to support vetting:

- Distribution of Vetting Support Requests (*e.g.*, visa or visa waiver applications) to Vetting Support Agencies;

[12] Adjudicators may consider many data points beyond Vetting Support Responses and the Analyst Recommendation in making an adjudication. For example, Adjudicators may consider information provided on a visa, travel, or benefit application by the individual, statements made by an individual during an interview at a port of entry or consulate, and the results of vetting performed outside of the NVC process. The NVC process is primarily focused on the review of classified national security information for vetting, but it is not intended to nor does it replace other types of vetting checks.

[13] Not all of the technologies used in the NVC processes are owned by the NVC or even DHS, but they are used to support and carry out the responsibilities of the NVC as put forth by NSPM-9.

- Receipt and distribution of Vetting Support Responses from Vetting Support Agencies to Adjudicating Agencies;
- Workflow management of Vetting Support Responses queued for review by Vetting Analysts;
- Integrated view-only capability to access records identified in Vetting Support Responses;
- Support for Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Managing access to data by individual users and infrastructure according to pre-determined rules and standards;
- Managing the retention of data according to approved record schedules;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for redress processes, Freedom of Information Act (FOIA) requests, discovery in litigation, and other data retrieval requirements.

Although records documenting the vetting that occurs through the NVC process are maintained using NVC technology, Adjudicating Agencies control and are responsible for those records. This Vetting Record includes the Vetting Support Request, Vetting Support Response, Analyst Notes, any recommendations from a Vetting Analyst, and Adjudicator's final decision. NVC technology allows Vetting Support Agencies to continue to maintain and control their information in their own systems while facilitating access by Adjudicating Agencies to Vetting Support Responses and other relevant information consistent with law and policy.

Individual Rights and Liberties

The NVC, in coordination with the DHS Chief Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties, has included in this PIA a discussion of civil rights and civil liberties raised by the creation of the NVC and its use of personally identifiable information (PII). The inclusion of an individual rights and liberties discussion in the PIA will improve transparency and assist the public in understanding the NVC and DHS's role in the NVC.

DHS is committed to the principles of due process, Constitutional protections, the fair and equal treatment of all individuals in its screening and vetting activities, and to ensuring the rights of all individuals while taking all lawful actions necessary to secure and protect the nation. In addition to the framework of protections and privacy mitigations detailed in this PIA, compliance with existing DHS policies will foster appropriate vetting uses of NVC processes and technologies for DHS actions and adjudications conducted by DHS personnel. For DHS vetting programs, this includes DHS personnel adherence to the existing DHS policy[14] that generally prohibits the consideration of race or ethnicity in investigating, screening, and law enforcement activities and

[14] For more information about these DHS policies, *see* https://www.dhs.gov/publication/department-homeland-security-commitment-nondiscriminatory-law-enforcement-and-screening and https://www.dhs.gov/publication/office-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.

limits the consideration of an individual's protected characteristics, and simple connection to a particular country, by birth or citizenship, as a screening criterion to situations in which such consideration is based on an assessment of intelligence and risk in which alternatives do not meet security needs. Accordingly, vetting activities conducted by DHS personnel using NVC processes and technologies may not be used to collect, access, use, or retain information on an individual solely on the basis of actual or perceived race, ethnicity, or nationality.

Privacy, Civil Rights, and Civil Liberties Protections

While enhancing the efficiency and effectiveness of Adjudicating Agencies' vetting activities, the NVC has established a variety of oversight, governance, and compliance mechanisms to ensure privacy, civil rights, and civil liberties protections are in place.

The NVC is overseen by the National Vetting Governance Board, a senior interagency forum that considers issues that affect the National Vetting Enterprise and the activities of the NVC and the IC Support Element. To ensure its activities and those of the NVC comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties, the Board has established a standing Legal Working Group and a separate standing PCRCL Working Group, both of which routinely review the activities of the NVC and advise the Board.

The NVC is supported by a full-time, dedicated Senior Legal Advisor, who serves as a liaison to the Legal Working Group and provides legal advice and counsel to the NVC concerning its various activities to ensure they comply with law, and a separate PCRCL Officer, who serves as a liaison to the PCRCL Working Group and provides dedicated support for all privacy, civil rights, and civil liberties issues arising in the context of the NVC. The PCRCL Officer's duties include ensuring the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of PII and working in coordination with the DHS Office for Civil Rights and Civil Liberties and other oversight offices to develop policy regarding privacy, civil rights, and civil liberties in connection with national vetting processes. The PCRCL Officer evaluates new or modified NVC technologies and ensures NVC compliance with the Privacy Act and other applicable privacy, civil rights, and civil liberties laws and policies including Executive Order 12333 and the Constitution.

The Office of the Director of National Intelligence has designated an Associate General Counsel and a Civil Liberties and Privacy Officer to support the IC Support Element. These officers work to ensure that the IC Support Element, like the NVC, conducts its activities in accordance with law and in a manner that protects individuals' privacy, civil rights, and civil liberties. They consult and coordinate with the NVC's Senior Legal Advisor and PCRCL Officer as well as all relevant NVC stakeholders, including representatives from the Legal and PCRCL Working Groups.

Additionally, the Adjudicating Agencies and Vetting Support Agencies that participate in the NVC process have internal oversight offices that address legal, privacy, civil rights, and civil liberties issues. These internal oversight offices are responsible for ensuring all Adjudicating Agency and Vetting Support Agency personnel comply with all relevant laws and policies.

The flow of information through the NVC process and technology is monitored to detect

events that may impact the integrity, confidentiality, or security of the information used. An event could include a suspected or confirmed privacy incident or breach. All events are reported promptly to the NVC Director, Senior Legal Advisor, and PCRCL Officer, as relevant and appropriate. The NVC, in coordination with other agencies, either investigates or monitors such events, and maintains awareness of and supports mitigation and remediation actions concerning such events. Notice of such events is provided to the National Vetting Governance Board and the Legal and PCRCL Working Groups, as necessary. Management, reporting, and notification related to these incidents will occur in accordance with applicable legal and policy requirements.

Access to information processed using NVC technology is restricted only to authorized users who have a need-to-know the information in the furtherance of their authorized missions and activities. For each vetting program facilitated by the NVC, the NVC coordinates with the Adjudicating Agency, the relevant Vetting Support Agencies, and the IC Support Element to define the appropriate data access rules for that program. This includes establishing prerequisites, such as training or security clearances for granting access to the data in question.

Ultimately, the Adjudicating Agency determines how long Vetting Records are stored, who can access that information using the NVC process and technology, and how the information is stored in its source systems. The specific requirements for and restrictions on data access will vary from one vetting program to the next. Additional detail on access controls is provided in the individual addenda to this PIA that describe separate vetting programs. User activity is logged and monitored for oversight and compliance purposes.

The U.S. Government ensures adequate redress mechanisms are in place to review complaints and requests from individuals impacted by vetting programs. Redress is an integral part of this commitment to ensuring privacy, civil rights, and civil liberties protections. The improved vetting processes implemented under NSPM-9 will be accompanied by a review of existing redress procedures to ensure that as vetting capabilities grow, agencies have processes in place to afford individuals opportunities for redress. Because the NVC does not itself adjudicate Vetting Support Requests, it will not establish its own redress system. Throughout the operations of the NVC, DHS's Office for Civil Rights and Civil Liberties and the DHS Privacy Office, corresponding offices in other Adjudicating Agencies, and DHS and component redress programs will review NVC plans and programs to ensure that adequate redress processes are in place for any vetting programs using the NVC process and technology.

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 President directed the establishment of the NVC as part of the National Vetting Enterprise in NSPM-9. The NSPM does not provide any new legal authority for the NVC (or any new authority to any participating agency) to collect, retain, store, or use information, nor does it

supplement or alter the existing adjudicative authorities and responsibilities of Adjudicating Agencies. All activities undertaken through the NVC process and technology are based on existing legal authorities for each participating agency.

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

Data used in the NVC process and technology remains under the control and stewardship of the Adjudicating Agency, with certain exceptions that allow a Vetting Support Agency to retain the data as described in Section 5.1. The System of Records Notices (SORNs) that apply to the records controlled by each participating agency for each vetting program will differ and are listed in the addenda of this PIA.

Depending on the nature of the vetting program and if U.S. citizen or lawful permanent resident information is included in the Vetting Support Requests compared against Vetting Support Agency holdings, a SORN established by the Vetting Support Agency may also apply.

Because the Privacy Act only applies to records about U.S. citizens and lawful permanent residents maintained in an agency system of records, SORNs may not govern or provide transparency on the use and sharing of data about other individuals. Additionally, the Judicial Redress Act extends certain protections of the Privacy Act to nationals of certain countries in some cases.

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

The Authority to Operate for the NVC technology was modified and approved in February 2022.

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

Each of the vetting programs that participate in the NVC must have an approved records retention schedule that covers all Vetting Records. The Vetting Support Agencies retain records maintained in their own systems according to their own approved retention schedules.

Although NVC technology may maintain Vetting Records, all records remain under the ownership of the Adjudicating Agency or Vetting Support Agencies. The NVC does not create any new data itself. The records used and created through the NVC processes will abide by the relevant agency's retention schedule.

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.

The provisions of the Paperwork Reduction Act are not applicable to the NVC, as no information is collected directly from members of the public. However, most information maintained by vetting programs is subject to the Paperwork Reduction Act. Vetting programs that use the NVC process and technology are outlined in the addenda of this PIA, and the Paperwork Reduction Act applicability is discussed there.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

The NVC coordinates agency vetting efforts to identify individuals who present a threat to national security, border security, homeland security, or public safety. A number of Adjudicating Agencies, each with different vetting programs, as well as Vetting Support Agencies will use the NVC process and technology to share information on these individuals. While individuals affected by each vetting program and the information shared will be different, as outlined in the addenda of this PIA, the type of information used through the NVC workflow can be described using the following categories: Vetting Support Requests, Vetting Support Responses, Analyst Notes, Analyst Recommendations, and Adjudications.

Vetting Support Requests

Adjudicating Agencies initiate Vetting Support Requests when they need to identify and analyze information that may be present in one or more Vetting Support Agency holdings to determine whether "individuals pose threats to national security, border security, homeland security, or public safety,"[15] in support of the U.S. Government's visa, naturalization, immigration benefit, immigration enforcement, travel, and border security decisions. For example, Vetting Support Requests may include applications for visas or visa waivers submitted by individuals seeking to travel or immigrate to the United States. The National Vetting Governance Board approves the NVC's support for any new vetting programs of Adjudicating Agencies.

Any vetting activity that occurs using the NVC process and technology will be initiated by a Vetting Support Request from an Adjudicating Agency. The information in a Vetting Support Request will differ based on what program is involved; more information is provided in the program-specific addenda to this PIA. Each Vetting Support Request generally also includes a Vetting Support Request ID number and metadata (*e.g.*, date and time received).[16]

Vetting Support Responses

Vetting Support Responses are generated in response to Vetting Support Requests. They

[15] *See* NSPM-9, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-optimizing-use-federal-government-information-support-national-vetting-enterprise/.
[16] This metadata is only used to ensure Vetting Support Responses are accurately linked within the NVC technology to the correct Vetting Support Requests and traceable to the Vetting Support Agency providing the response.

indicate whether Vetting Support Agency holdings, which may include intelligence, law enforcement, or other information, contain potentially relevant and appropriate records related to the adjudication at issue. The Vetting Support Responses include links or pointers to information that Vetting Support Agencies assess are valid and analytically significant identity matches. These links or pointers allow Analysts to view related information in other (typically classified) systems to which the Analyst has authorized access. Originally, the Vetting Support Responses only included these links or pointers which meant that analysts had to search other systems to access additional information. Now, the Vetting Support Agencies may also provide relevant information from the Vetting Support Request that matches information in Vetting Support Agency holdings. Unlike the links or pointers information, this matched information is presented for analysts to view in the NVC technology; however, analysts will still need to access other systems outside of the NVC technology to view all relevant information from Vetting Support Agency holdings. The Vetting Support Responses typically include the Vetting Support Request ID number and metadata as well.

Analyst Notes

Analysts Notes are created by Vetting Analysts when making a recommendation on a Vetting Support Request. They capture the analysis performed by the Vetting Analyst of the information found in Vetting Support Agency holdings. Analyst Notes are made available to the Adjudicator when possible and appropriate, depending on the vetting program.

Analyst Recommendations

Analyst Recommendations are generated by Adjudicating Agency Vetting Analysts. They typically contain the Vetting Support Request ID number, metadata, and the Vetting Analyst's recommendation to an Adjudicator (*e.g.*, approve, deny). An example of an Analyst Recommendation is the recommendation to approve a visa waiver request.[17]

Adjudications

Adjudications are the decision made by an Adjudicator on the matter in question after all vetting, including any vetting conducted outside the NVC process, is complete. The specific nature of Adjudications may vary among vetting programs. An example of an Adjudication is the decision to grant a visa.

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

The initial source of information for the NVC process is the Adjudicating Agency, which electronically delivers the Vetting Support Request from its internal system either directly to the Vetting Support Agency(s) that support its vetting program or to the NVC, which can facilitate

[17] Some Adjudicating Agencies may determine certain Vetting Support Responses will not require review by a Vetting Analyst, and therefore they will not result in the creation of an Analyst Recommendation or the creation of Analyst Notes. This creates efficiencies in the review and adjudication process when certain thresholds are met.

delivery to the appropriate Vetting Support Agency(s) using NVC technology.[18] The Vetting Support Response is then delivered to the NVC technology, typically from the Vetting Support Agency's own information system.

The Vetting Analyst then conducts analysis of the Vetting Support Responses to generate the Analyst Notes and Analyst Recommendation, which are recorded in the NVC technology. The NVC technology also electronically delivers the Analyst Recommendation to an Adjudicating Agency system, where Adjudicators access and review them as part of their Adjudications. Each Adjudicating Agency determines the standards for information upon which Adjudicators rely to inform their decisions. According to agency requirements, Adjudicators may also use the NVC technology to access Vetting Support Responses before making a decision.

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

The NVC itself will not use commercial sources or publicly available data as part of the vetting process. However, Adjudicating Agencies and Vetting Support Agencies that use the NVC process and technology for a particular vetting program may use commercial sources and publicly available data consistent with their own authorities and policies as part of their internal processes.

2.4 Discuss how accuracy of the data is ensured.

Adjudicating Agencies are responsible for ensuring that Vetting Support Requests are complete and accurate when introduced to the NVC process and technology. The NVC technology provides sufficient technical measures to maintain data integrity and quickly identify data problems (such as data corruption) should they occur. If the delivery of the Vetting Support Request occurs by the Adjudicating Agency directly to the Vetting Support Agency(s), then the Adjudicating Agency is responsible for ensuring the transmittal occurs in a manner that protects the integrity of the data. Similar technical measures are used to ensure the integrity of Vetting Support Responses, Analyst Recommendations, and Adjudications transmitted using the NVC technology.

The NVC facilitates discussions among Adjudicating Agencies and Vetting Support Agencies about data integrity within the technical processes. Risks to data integrity, such as data latency, are considered and the technical solutions architected seek to minimize such risks. In some vetting programs, for example, a Vetting Support Request may be able to be updated by the individual or by the Adjudicating Agency with new or different data while vetting activities are ongoing. In these instances, it is important that the Vetting Support Request be promptly updated with the Vetting Support Agencies and in the NVC technology so that Adjudications are based on the most current information available. Each vetting program may present different or unique risks

[18] For example, the Vetting Support Request could contain all applicant-provided information an individual submitted to an Adjudicating Agency for a specific benefit. The source of information for this initial data is generally the individual applying for the benefit, but the source(s) may vary depending on the specific vetting program. This original collection of information is covered by the source system PIA and SORN. For DHS, all source system PIAs and SORNs can be found here: https://www.dhs.gov/privacy.

to data accuracy, so the solutions architected may not always be the same for each program. Data accuracy issues specific to each vetting program are discussed in the relevant addendum to this PIA.

Additionally, Vetting Analysts and Adjudicators conduct manual reviews of the information presented to them prior to making any recommendation or adjudication. These individuals use all information available to them (*e.g.*, Analyst Recommendation, Analyst Notes if available, Vetting Support Responses and associated records) to ensure they have an accurate accounting of a Vetting Support Request before a decision is made. This additional layer of manual review helps maintain data accuracy throughout the NVC workflow.

Vetting Support Agencies that are elements of the Intelligence Community will conduct all NVC analytic support activities in accordance with Intelligence Community Directive 203, *IC Analytic Standards*,[19] which represent the core principles of intelligence analysis and are applied across the IC or other applicable analytic standards employed by each Vetting Support Agency. As such, all Vetting Support Agency analytic products shall be consistent with the five Analytic Standards requiring the products to be objective, independent of political consideration, timely, based on all available sources of intelligence, and implement and exhibit specific Analytic Tradecraft Standards. Additionally, Vetting Support Agencies will apply *The Principles of Professional Ethics for the Intelligence Community*, which reflect the core values common to all IC elements, regardless of individual role or agency affiliation.[20]

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that changes or corrections made to PII in the underlying Adjudicating Agency source systems will not be updated or pushed to the Vetting Support Agencies, leading to inaccurate or out-of-date information being reviewed for vetting.

Mitigation: This risk is partially mitigated. Protocols are in place to ensure that information in the Vetting Support Request is updated during the vetting processes to ensure the most recent information available is used for vetting; however, the U.S. Government has a need to maintain a record of any decision that affects an individual, and that record should contain and point to the information that was relied upon at the time. If it is later determined that some of that information was incorrect, the original record should not be modified, but rather annotated to indicate the inaccurate data and the new, correct information. Inaccurate data would not be erased, but it must be clear from the totality of the updated record which data was found to be inaccurate and which is correct.

Privacy Risk: There is a risk that Vetting Support Responses do not correctly match the individual associated with a specific Vetting Support Request due to misidentification.

Mitigation: The NVC has taken appropriate steps to mitigate this risk. It is anticipated that information in most vetting programs will be collected directly from the individuals to whom that

[19] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.
[20] *See* www.dni.gov/index.php/how-we-work/ethics.

information pertains, which should ensure a high level of accuracy upon collection. In some cases, information will be collected about an individual from a third-party, such as in the case of a visa applicant providing information in the application about family members or individuals in the United States they plan to visit or who will employ them.

Vetting programs collect a number of identifiers and other information about an individual, which increases the likelihood of accurately matching individuals between Vetting Support Requests and Vetting Support Responses. Collection of this information assists both the Vetting Support Agencies and the Vetting Analysts in determining any possible misidentification issues prior to adjudication. For example, if previous history of travel to the United States is collected, then that information can be used to confirm an identity match.

Vetting Support Agencies have their own internal processes in place to ensure accurate information is distributed back to Adjudicating Agencies. This includes sharing information in accordance with Intelligence Community Directive 203, *IC Analytic Standards*. Additionally, Vetting Support Agencies review all information to ensure it is appropriate to be shared outside of their own agency.

As vetting programs are added to the NVC process, any additional and unique risks of misidentification for each vetting program will be discussed in the addenda of this PIA.

Privacy Risk: The NVC technology requires the transfer of Vetting Records to and from several systems and across varying levels of network security (*i.e.*, classified to unclassified, and the reverse). This may introduce a greater risk of the data being corrupted by errors or weaknesses in technical processes, leading to inaccurate data.

Mitigation: This risk is mitigated. Technical measures are in place to ensure data integrity is not affected during transmittals among systems and across security levels. For example, tools that validate record content and record counts are used to quickly identify data problems (such as data corruption) should they occur. Additionally, Vetting Support Agencies will provide an electronic notification to the NVC if they encounter data quality issues related to a Vetting Support Request, which the NVC will then coordinate with the Adjudicating Agency for resolution, if applicable.

Privacy Risk: There is a risk the NVC technology will not have appropriate security safeguards, putting individual PII at risk of breach or compromise.

Mitigation: This risk is mitigated. Because the NVC technology is being maintained on a classified network, DHS follows the information technology security requirements established in DHS's *Sensitive Compartmented Information Systems* 4300C *Instruction Manual*; National Institute of Standards and Technology Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; and Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*. The NVC technology must also receive an Authority to Operate, which requires approval by the DHS Chief Information Security Officer and DHS Chief Privacy Officer. Other agencies participating in the NVC process apply and follow comparable standards with respect to their information technology systems.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The NVC has been established to implement "an integrated approach to use data held across national security components" for the purpose of "determining whether individuals pose threats to national security, border security, homeland security, or public safety."[21] The technology, tools, and processes offered by the NVC support Adjudicating Agencies' need for access to intelligence, law enforcement, and other information, much of which is classified, to make fully-informed decisions.

Vetting Support Agencies use the initial information provided by Adjudicating Agencies in Vetting Support Requests to generate a Vetting Support Response.

Vetting Analysts use the Vetting Support Responses and the information available via links or pointers to other Vetting Support Agency systems, as appropriate, to make a recommendation to Adjudicators at their home agency.

Adjudicators use the Analyst Recommendation, and any other information authorized by the Adjudicating Agency, to make a decision on the pending matter and record that as the Adjudication (*e.g.*, approve, deny). Depending on the vetting program and the Vetting Support Request, the Adjudicators may also use the information in Vetting Support Responses, including the information available via links to other Vetting Support Agency systems, to make their decision.

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.

No. The NVC does not conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

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

Yes. Any DHS Component vetting programs that participate in the NVC will have personnel, specifically Vetting Analysts and Adjudicators, who are assigned roles and responsibilities using the NVC technologies and other systems used to support vetting. Additionally, depending on which Adjudicating Agencies and vetting programs external to DHS are on-boarded to the NVC, personnel from those agencies will have access to and roles within the NVC technologies and other systems used to support vetting.

3.4 Privacy Impact Analysis: Related to the Uses of Information

[21] *See* NSPM-9, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-optimizing-use-federal-government-information-support-national-vetting-enterprise/.

Privacy Risk: There is a risk that the stated purposes of the collection of data are inconsistent with the vetting activities that will be occurring using the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of the Vetting Support Request data, as documented in SORNs, PIAs, Privacy Act Statements or Privacy Notices, and information sharing agreements, will be reviewed as a part of the NVC process to on-board a new vetting program to ensure they are accurate and adequately support the vetting activities. This will help to ensure that individuals who provide the information receive adequate public notice of the purposes for collection and uses of the data.

Privacy Risk: There is a risk that the information collected through the NVC process will be used inappropriately by users of the NVC technology.

Mitigation: This risk is mitigated. The NVC has implemented audit capabilities and access controls to ensure that only those who should have access to the information are granted such. Additionally, information sharing agreements will be reviewed and modified, if applicable and necessary, to ensure that they support NVC vetting activities and privacy and civil rights and civil liberties protections.

Each vetting program is also reviewed by the Legal and PCRCL Working Groups to ensure all legal, privacy, civil rights, and civil liberties requirements, including those pertaining to use of information in support of that program, are met. After these reviews, the National Vetting Governance Board ultimately approves whether any new vetting program is on-boarded to the NVC workflow.

Privacy Risk: There is a risk that the NVC will share information with Vetting Support Agencies that do not have authority to support vetting activities for a specific vetting program or do not have data relevant to Adjudicating Agencies based on the applicable legal standards.

Mitigation: This risk is mitigated. The Legal Working Group and the PCRCL Working Group supporting the National Vetting Governance Board are charged with advising the activities of the Board and ensuring the NVC complies with applicable law and appropriately protects individuals' privacy, civil rights, and civil liberties. The Working Groups have conducted a thorough review of the Implementation Plan for the NVC and engaged in reviewing the NVC's technical designs, plans, and deployment to ensure they meet all legal and PCRCL requirements. These reviews include an evaluation of each vetting program incorporated in the NVC process and technology to ensure the incorporation of that program does not exceed the legal authorities of either the Adjudicating Agency or the Vetting Support Agencies.

Additionally, any information sharing agreements for a particular vetting program between an Adjudicating Agency and Vetting Support Agency will be reviewed and modified, if applicable and necessary, to ensure that they support NVC vetting activities and privacy, civil rights, and civil liberties protections.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information

collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This PIA and its addenda provide notice of the privacy risks related to the NVC and how the information in the NVC process will be used. The NVC itself does not and cannot provide direct notice to individuals that their information will be used and processed by the NVC because it does not interface with individuals who are vetted.

For individual vetting programs, the Adjudicating Agencies are responsible for determining and delivering appropriate notice to individuals from whom information is collected and incorporated into a Vetting Support Request. These agencies may decide to provide new or modify existing notices to individuals at the point of collection or other forms of notice such as a SORN or PIA to provide greater transparency about the nature of vetting activities that occur using their information. That decision is reserved to the Adjudicating Agency. The Legal and PCRCL Working Groups, however, may review notices for a vetting program and make suggestions or recommendations for the Adjudicating Agencies to consider.

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

Depending on the vetting program, individuals may have the opportunity to decline to provide the information used in a Vetting Support Request. The notice provided to the individual by the Adjudicating Agency at the point of collection will specify for the individual what options exist related to consent, opt-in, or opt-out.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may be unaware of the NVC, its purpose, how it operates, and what the potential impacts it has on individuals and their data. Individuals also may not have a full understanding of where their data is going and how it is used by the NVC.

Mitigation: This risk cannot be fully mitigated. Due to the sensitive nature of intelligence, law enforcement, and other information incorporated into vetting activities through the NVC process and technology, it may not be possible for individuals to be informed when their information is used in the NVC process and technology. The NVC, at the direction of the National Vetting Governance Board, is taking a number of measures to provide transparency in other forms. This PIA and subsequent addenda provide information and assess the privacy risks that use of the NVC process and technology poses generally and to affected individuals for particular vetting programs. Also, the National Vetting Governance Board will publicly release an unclassified version of the NVC Implementation Plan. The NVC engages in significant public outreach efforts to promote better understanding of the NVC among oversight entities such as congressional committees, the

media, and public interest groups.

When new vetting programs join the NVC process, specific notice will be given, as appropriate. For example, the privacy compliance documentation (*e.g.*, PIA, SORN) for those vetting programs may be updated, Privacy Act Statements or Privacy Notices may be amended on the forms which are the initial instruments for the data collection, and any changes to an individual application form submitted for a benefit will require a Paperwork Reduction Act notice.

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Because the Vetting Support Agencies and Adjudicating Agencies each have different authorities and the vetting programs will be governed by different SORNs, the retention periods for each will be different. The retention of the data is determined on a program-by-program basis based on the authorities of the Adjudicating Agency that owns and controls the data in the vetting program and the Vetting Support Agencies with which the data is shared. If a Vetting Support Agency identifies Vetting Support Request information as retainable in accordance with applicable information sharing agreements and its Attorney General Guidelines for the protection of U.S. person information, that individual record may be retained for a longer period in accordance with those agreements and that Vetting Support Agency's individual authorities to retain that information. The retention period for each vetting program is outlined in the addenda of this PIA.

The Legal and PCRCL Working Groups as well as the privacy and civil liberties oversight offices for the Adjudicating Agencies and Vetting Support Agencies review and evaluate retention periods for vetting programs that are being added to the NVC to ensure those periods are appropriate. After these reviews, the National Vetting Governance Board receives input from the Working Groups related to any risks or issues, including retention policies, before ultimately approving any new vetting program for incorporation in the NVC process.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that some individuals within a vetting program may gain U.S. Person status during the recurrent vetting period and continue to be vetted.

Mitigation: The risk is partially mitigated. Upon discovery of status change during Vetting Support Agency's manual review, the identified record is then handled in accordance with the Vetting Support Agency's Executive Order 12333 Attorney General Guidelines. Additionally, the NVC Privacy, Civil Rights, and Civil Liberties Officer will review initiatives underway within DHS with the goal of better assessing an individual's status and disseminating information when an individual changes status, such as when an individual becomes a U.S. Person. Such sharing of information is important for removing individuals from recurrent vetting once they have changed or adjusted status.

Privacy Risk: There is a risk that Vetting Support Agencies will retain information from Vetting Support Requests for longer than is necessary.

Mitigation: This risk is mitigated. Existing and new information sharing agreements between Adjudicating Agencies and Vetting Support Agencies that define the retention of data are reviewed by the Legal and PCRCL Working Groups prior to the on-boarding of any new vetting programs to the NVC process. These information sharing agreements are reviewed along with retention periods outlined in applicable PIAs, SORNs, record retention schedules, and Attorney General Guidelines. These reviews aim to ensure retention policies are appropriate and balance the U.S. Government's need to retain the data for operational reasons and afford effective redress against the risks to individuals that lengthy retention periods can create (*e.g.*, data breaches and the possible adverse consequences of relying on aging, inaccurate data).

Additionally, the retention period for the Vetting Support Records applicable to each vetting program is documented internally in classified documents that outline the processes for those particular vetting programs. This documentation defines the authorized retention period of Vetting Support Requests shared with Vetting Support Agencies and the purposes for such sharing. Vetting Support Agencies may retain Vetting Records for longer periods when, for example, they are identified as foreign intelligence or are relevant to law enforcement investigations in accordance with existing information sharing agreements, law, and policy.

For Vetting Support Request information ingested by Vetting Support Agencies into their internal systems, this risk is not fully mitigated solely by NVC technologies. This risk is instead further mitigated by the internal retention controls of the Vetting Support Agencies, to include the record retention schedules, the National Security Act, and Executive Order 12333-derived retention limitations.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government and private sector entities.

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.

Yes. For each vetting program, the NVC technology facilitates the sharing of information between and among Vetting Support Agencies and Adjudicating Agencies. Each vetting program, along with the corresponding Adjudicating Agency, is outlined in the addenda of this PIA.

The information is shared and accessed through the NVC workflow processes described in the Overview and Sections 2.0 and 3.0. Each of the Vetting Support Agency and Adjudicating Agency has different systems and technical processes that will connect to the NVC technology to facilitate the flow of data during the NVC process.

Because vetting programs may contain information involving Special Protected Classes of individuals, special sharing and handling requirements may need to be implemented as part of the NVC process and technology for a particular vetting program.[22] The NVC and Vetting Support Agencies will implement the appropriate safeguards needed to properly identify and display Special Protected Classes data to allow users to properly execute the applicable sharing requirements and restrictions. Training related to the data for particular vetting programs and any special restrictions on handling, use, and disclosure of that data, including Special Protected Classes data, will also be provided to Adjudicating Agency and IC Support Element personnel who participate in the NVC process.

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

Because Vetting Support Agencies and Adjudicating Agencies each have different authorities and vetting programs will be governed by different SORNs, the compatibility of the external sharing to be performed through the NVC processes will be analyzed on a program-by-program basis. This will be outlined for each vetting program in the addenda of this PIA.

Before on-boarding with the NVC, each vetting program is reviewed by the Legal and PCRCL Working Groups to evaluate if existing information sharing agreements (or other similar documentation) and routine uses of applicable SORNs are sufficient or if modifications are required. After these reviews, the National Vetting Governance Board ultimately decides whether to integrate a new vetting program into the NVC process.

6.3 Does the project place limitations on re-dissemination?

The re-dissemination limitations of the information shared through the NVC process will vary for each vetting program. NVC internal documentation for that vetting program, as well as information sharing agreements between the Adjudicating Agency and Vetting Support Agencies, will outline these requirements.

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

All of the systems used throughout the NVC process maintain logs of the information shared between agencies.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be inappropriately shared between Adjudicating Agencies and Vetting Support Agencies.

Mitigation: This risk is mitigated. Each vetting program is reviewed by the Legal and

[22] *See* 8 U.S.C. § 1367, "Penalties for unauthorized disclosure of information of special protected classes," *available at* https://www.gpo.gov/fdsys/pkg/USCODE-2011-title8/pdf/USCODE-2011-title8-chap12-subchapII-partIX-sec1367.pdf.

PCRCL Working Groups to ensure information sharing arrangements, documented in agreements or otherwise, are sufficient for that vetting program's scope and mission. The specific sharing arrangements for each vetting program may be described in further detail in the addenda of this PIA.

Additionally, all sharing of data is documented through audit logs that are reviewed to ensure no inappropriate sharing occurs. Any inappropriate sharing of information by personnel of Adjudicating Agencies or Vetting Support Agencies would be subject to disciplinary action in accordance with the policies of those agencies.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

The NVC does not exercise any legal authority to collect, retain, use, or share information. It does not own or control any of the Vetting Records, but rather provides the technology through which the records are transmitted and maintained. Therefore, the NVC does not receive or have the authority to determine individual requests for access.

Generally, individuals should refer to the applicable PIA and SORN of the vetting program to determine the procedures that allow individuals to access their information. The relevant addendum to this PIA identifies the applicable SORN and PIA for each vetting program.

The NVC will forward any request for data incorporated in the NVC process and technology, including requests under the Privacy Act, FOIA, or Judicial Redress Act, to the appropriate Adjudicating Agency or Vetting Support Agency exercising control over the record for disposition. NVC staff will work with IC Support Element personnel and any Adjudicating Agency or Vetting Support Agencies receiving referrals from the NVC for record requests to ensure the response to such requests is coordinated and consistent with legal requirements.

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

The NVC itself does not possess the legal authority to collect, retain, use, or share information. Accordingly, the NVC does not provide any specific redress process. Instead, Adjudicating Agencies establish and operate any redress processes necessary or appropriate to review their adjudications. The NVC, does however, provide a capability, both in a shared physical space and through virtual connectivity, to support Adjudicating Agencies and Vetting Support Agencies in processing redress complaints related to vetting activities that were conducted through the use of the NVC process and technology. The roles of the different personnel involved in the redress process may vary by vetting program and are therefore documented in the relevant

addendum for that vetting program.

Individuals should also refer to the applicable PIA and SORN for the vetting program to determine the procedures that allow individuals to correct inaccurate or erroneous information.

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

Individuals can identify the procedures for correcting their information for a particular vetting program by reviewing the program's applicable PIA and SORN, as well as the relevant addendum in this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the NVC technology may not support the production of Vetting Records to an individual in response to a request or support a request to review vetting to correct inaccurate information.

Mitigation: This risk is mitigated. The NVC technology is designed to support the requirement to be able to access Vetting Records to process FOIA requests and redress inquiries. Any corrections will be made in systems owned by the Vetting Support Agency(s) or the Adjudicating Agency, and changes pushed through the NVC technology.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

The NVC will oversee the conduct of internal compliance reviews at regular intervals to ensure that privacy, civil rights, and civil liberties requirements are met on an ongoing basis. The types of reviews that will be conducted include reviews of technical reports that document the frequency and nature of data errors; reviews of the NVC technology to ensure that it is functioning as intended; reviews to ensure that U.S. persons and Special Protected Classes are being accurately identified in accordance with applicable requirements; reviews of user and system administrator roles to ensure appropriate privileges and access to data are being implemented; reviews to ensure all required trainings have been completed by users of the NVC technology; reviews to ensure that the NVC technology is accurately tracking retention periods for records; and reviews of the NVC technology's audit trails to validate that the required user activity is being captured. These reviews also require the participation and cooperation of the IC Support Element, Vetting Support Agencies, and Adjudicating Agencies. Outcomes of the reviews are briefed to the Director of the NVC, the IC Support Element, the Legal and PCRCL Working Groups, and the National Vetting Governance Board, as appropriate.

8.2 Describe what privacy training is provided to users

either generally or specifically relevant to the project.

Training is required for all individuals using the NVC technology. Additional training may be required for specific vetting programs or information contained therein. Any such additional training is described in the relevant addendum for that vetting program.

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

Decisions about access to the data for each vetting program that is incorporated in the NVC process are coordinated with the PCRCL and Legal Working Groups, with the Adjudicating Agency and applicable Vetting Support Agencies determining these requirements. Once decisions are made concerning the access controls for different categories of users, those decisions are documented and written procedures are developed for how those privileges will be granted, managed, and subject to review by oversight offices. Specifics concerning the access controls, permissions, and data tags for particular vetting programs will vary. Accordingly, additional details are provided in the addendum for each vetting program.

The NVC facilitates vetting under Adjudicating Agencies' existing legal authorities by offering a process and technology that provides access to appropriate intelligence and information held by Vetting Support Agencies. Adjudicating Agency personnel have access to NVC technology, but remain under the operational control of their own agencies, operate under their agencies' authorities, and maintain access to their agencies' data and systems.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Each vetting program is reviewed by the Legal and PCRCL Working Groups to ensure information sharing and other legal, privacy, civil rights, and civil liberties requirements are sufficient. After these reviews, the National Vetting Governance Board ultimately decides whether to incorporate any new vetting program into the NVC process.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: There is a risk that the use, access, and sharing of PII through the NVC process and technology may not be auditable to demonstrate compliance with privacy principles, relevant laws, and the standards described in this PIA and other documentation.

Mitigation: This risk is mitigated. Technical mechanisms facilitate oversight of users who can access data using NVC technology, allowing for the review of audit data to identify potential misuse. Decisions about access to the data are facilitated through the PCRCL and Legal Working Groups for each vetting program that joins the NVC. Data tagging of Vetting Support Requests and

Vetting Support Responses helps to ensure that records and data are technically managed in compliance with those decisions. Data tags are used to ensure appropriate management of data that is subject to different restrictions on use, access, sharing, and handling. Data tags manage access privileges for different user groups, U.S. person or Specially Protected Classes data, and law enforcement information. Data tagging requirements vary by vetting program and are reviewed by the PCRCL and Legal Working Groups.

Privacy Risk: There is a risk that auditing standards will vary from Adjudicating Agency to Adjudicating Agency, depending on what they choose to adopt, leading to inconsistent levels of accountability and protections for individuals and their data.

Mitigation: This risk is mitigated. The PCRCL Working Group has established minimum auditing standards for users of the NVC technology - specifically, a core set of user activities that is captured in an audit log. It is possible that for a particular vetting program, an Adjudicating Agency may wish to expand the type of data captured in user audit logs. But in no case will user audit logs capture less information than the standards set by the NVC.

Privacy Risk: There is a risk that, once deployed, the NVC process and technology used will evolve or differ from what is documented in this PIA and other documents on which PCRCL analysis was based.

Mitigation: This risk is mitigated. The NVC has prepared a classified Concept of Operations (CONOP) with addenda for each vetting program that joins the NVC process. The CONOP must be approved by the National Vetting Governance Board (following review by the Legal and PCRCL Working Groups) prior to implementation. Any material operational changes or on-boarding of new vetting programs requires documentation for review by the Legal and PCRCL Working Groups and approval by the National Vetting Governance Board. Additionally, the PCRCL Officer will ensure this PIA is updated, as required.

Responsible Officials

Monte Hawkins
Director
National Vetting Center
Department of Homeland Security

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

NVC PIA Addendum Quick Reference Guide

1. **NVC PIA Addendum 1: U.S. Customs and Border Protection's (CBP) Electronic System for Travel Authorization**
2. **NVC PIA Addendum 2: Vetting in Support of Enduring Welcome (EW)**
3. **NVC PIA Addendum 3: United States Refugee Admissions Program (USRAP)**
4. **NVC PIA Addendum 4: Advance Travel Authorization (ATA)**
5. **NVC PIA Addendum 5: U.S. Department of State's (State) Non-Immigrant Visa (NIV)**
6. **NVC PIA Addendum 6: U.S. Citizenship and Immigration Services (USCIS) Asylum Program (UAP)**
7. **NVC PIA Addendum 7: U.S. Department of State's (State) Immigrant Visa (IV)**

NVC PIA Addendum 1:

U.S. Customs and Border Protection's (CBP) Electronic System for Travel Authorization (ESTA)

Last updated May 12, 2022 (back to top)

The U.S. Customs and Border Protection's (CBP) Electronic System for Travel Authorization (ESTA)[23] is a web-based application and screening system used to determine whether citizens and nationals from countries participating in the Visa Waiver Program (VWP)[24] are eligible to travel to the United States. Applicants use the ESTA website to submit biographic information, along with U.S. point of contact information, and respond to questions related to an applicant's eligibility to travel under the VWP. ESTA information is necessary to issue a travel authorization consistent with the requirements of Form I-94W. A VWP traveler who intends to arrive at a U.S. port of entry must obtain an approved travel authorization via the ESTA website prior to entering the United States. The ESTA program allows CBP to eliminate the requirement that VWP travelers complete Form I-94W prior to being admitted to the United States because the ESTA application electronically captures duplicate biographical and travel data elements collected on the paper Form I-94W.

ESTA collects and maintains records on nonimmigrant aliens and other persons, including U.S. citizens and lawful permanent residents, whose names are provided to DHS as part of a nonimmigrant alien's ESTA application. An applicant's eligibility to travel to and enter the United States is determined by vetting his or her ESTA application information against selected security and law enforcement databases at DHS, including TECS[25] and the Automated Targeting System (ATS).[26] In addition, ATS retains a copy of ESTA application data to identify individuals from VWP countries who may pose a security risk. ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems. CBP may also vet ESTA application information against security and law enforcement databases at other federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States and is eligible to travel to and enter the United States under the VWP. The results of this vetting may inform CBP's assessment of whether the applicant's travel poses a law enforcement or security risk and whether the application should be approved.[27]

---

[23] *See* DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA) and subsequent updates, *available at* https://www.dhs.gov/privacy.

[24] *See* 8 CFR 217. The Visa Waiver Program (VWP), administered by DHS in consultation with the Department of State, permits citizens of certain countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those 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.

[25] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* https://www.dhs.gov/privacy.

[26] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS) and subsequent updates, *available at* https://www.dhs.gov/privacy.

[27] Approved ESTA applications are valid for a maximum of two years (depending on the VWP country), or until the passport expires, whichever comes first. Approved ESTA applications support multiple trips a traveler may make to

ESTA applicant information may be shared either in bulk or on a case-by-case basis. Routine Use G in the ESTA SORN[28] outlines that DHS may share information stored in ESTA in bulk as well as on a case-by-case basis with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies to vet against the other agency's databases to identify violations proactively. CBP documents ongoing, systematic sharing with partners, including documenting the need to know, authorized users and uses, and the privacy protections that will be applied to the data.

With the publication of this PIA and addendum, ESTA will be the first vetting program to conduct vetting using the National Vetting Center (NVC) process and technology. This ESTA vetting will augment, but not replace the vetting activities described above using ATS and other systems.[29] The NVC process and technology described in the full NVC PIA above will be used to facilitate the vetting of ESTA application data, helping to ensure CBP is informed by all appropriate responsive information held by ESTA Vetting Support Agencies.

The starting point for ESTA vetting of all ESTA applicants through the NVC process and technology is the transmission of an ESTA Vetting Support Request, which consists of ESTA application data, to the ESTA Vetting Support Agencies.[30] Existing memoranda of agreement between CBP and the various ESTA Vetting Support Agencies determine which data fields in the ESTA application are included in the Vetting Support Request, and how they are delivered, to each ESTA Vetting Support Agency. CBP Vetting Analysts use NVC technology to receive and review any ESTA Vetting Support Request for which there is a relevant and appropriate classified or unclassified record made available by the ESTA Vetting Support Agencies. CBP Vetting Analysts develop a recommendation to either grant or deny the ESTA based on their analysis of this information. CBP Adjudicators then review the recommendation and Analyst Notes, if any, provided by the CBP Vetting Analyst along with any additional, unclassified information available to make their final decision to grant or deny the ESTA application.

The NVC's process and technology will allow for the:

- Distribution of Vetting Support Requests (*i.e.*, data from all ESTA applications) to ESTA Vetting Support Agencies;
- Receipt and distribution of Vetting Support Responses from ESTA Vetting Support Agencies to CBP;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for CBP Vetting Analysts to access classified and unclassified records identified by an ESTA Vetting Support Agency as relevant to a Vetting Support Request;

---

the United States without having to re-apply for another ESTA. For more general ESTA information, *see* http://www.cbp.gov/travel/international-visitors/esta.

[28] DHS/CBP-009 Electronic System for Travel Authorization, 81 FR 43462 (September 2, 2016).

[29] The on-boarding of ESTA as the first vetting program to the NVC process does not constitute new vetting for ESTA applicants, but is rather a new process being established for existing vetting activities.

[30] As explained in the PIA, the NVC does not make recommendations or adjudications. Its role is limited to that of facilitator or service provider of the NVC process and technology used to facilitate vetting by CBP.

- Support for CBP Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Managing access to data by individual users and infrastructure according to pre-determined rules and standards;
- Managing the retention of data according to approved ESTA record schedules and information sharing agreements;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for ESTA redress processes, FOIA requests, discovery in litigation, and other data retrieval requirements.

(Update: May 12, 2022) Department of State Access to ESTA Data in the NVC for Non-Immigration Visa Vetting

Upon implementation of the Department of State's (State) Non-Immigrant Visa (NIV) program at the NVC, State Vetting Analysts will have read-only access to all denied ESTA vetting records, including CBP Vetting Analyst and Adjudicator notes, within the NVC technology to support the NIV program. ESTA applicants that are denied authorization for travel to the United States under the VWP are instructed that they may apply for a visa. Accordingly, State expects that many visa applicants from VWP countries will have previously applied for an ESTA. Therefore, State will utilize information contained in ESTA vetting records within the NVC technology to further their analysis of pending NIV applications, as appropriate. Additional information regarding the NIV program and State Vetting Analysts access to ESTA data is detailed in NVC PIA NIV Addendum below.

Privacy Impact Analysis

Authorities and Other Requirements

CBP collects ESTA application information pursuant to 8 U.S.C. § 1187, which authorizes the Secretary of Homeland Security, in consultation with the Secretary of State, to "develop and implement a fully automated electronic travel authorization system to collect such biographical and other information as the Secretary of Homeland Security determines necessary to determine, in advance of travel, the eligibility of, and whether there exists a law enforcement or security risk in permitting, the alien to travel to the United States." The creation of the NVC does not provide any new legal authorities to CBP to collect, retain, store, or use information, or to make adjudications based on vetting. All activities undertaken through the NVC process are based on CBP's existing legal authorities. ESTA Vetting Support Agencies similarly are engaged in the vetting process pursuant to their existing legal authorities.

SORN coverage for ESTA activities is provided by DHS/CBP-009 Electronic System for Travel Authorization and DHS/CBP-006 Automated Targeting System.[31]

[31] DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 81 FR 60713 (September 2, 2016) and DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012). DHS's Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally*

Characterization of the Information

CBP will continue to collect the same information from ESTA applicants through the application process. However, in order to make the final ESTA adjudication, CBP Adjudicators will now receive an Analyst Recommendation. This recommendation is generated by the CBP Vetting Analysts who, acting under CBP authorities, analyze information made available by ESTA Vetting Support Agencies. The nature and scope of information that is made available by the ESTA Vetting Support Agencies is defined by the vetting and information sharing agreements in place between CBP and those agencies, and the classified NVC Concept of Operations (CONOP). This includes terrorism information provided by the Office of the Director of National Intelligence's (ODNI) National Counter Terrorism Center (NCTC).[32]

Privacy Risk: There is a risk that CBP may make decisions to grant or deny an ESTA application based on inaccurate information identified during the NVC process.

Mitigation: This risk cannot be fully mitigated. Information is collected directly from applicants during the ESTA application process, ensuring a high level of accuracy upon collection. However, if an ESTA applicant provides inaccurate information, it may result in inaccurate results from the NVC process. When information is provided by the ESTA applicant, ESTA Vetting Support Agencies are required to apply their analytic standards to ensure that information regarding the ESTA applicant is objective, timely, relevant, and accurate. For example, ESTA Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive 203, which requires that PII is disseminated "only as it relates to a specific analytic purpose . . . [and] consistent with IC element mission and in compliance with IC element regulation and policy, including procedures to prevent, identify, and correct errors in PII."[33] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any factors affecting source quality and credibility.[34]

The recommendations provided by the CBP Vetting Analysts inform but do not determine the outcome of an ESTA application. It is the responsibility of CBP to evaluate the substance and assessed reliability of the additional information provided by the ESTA Vetting Support Agencies, in conjunction with other information available to the CBP Adjudicator in determining whether to approve or deny an ESTA application.

Privacy Risk: There is a risk that CBP Adjudicators will make ESTA adjudications based solely on the Analyst Recommendation and not all of the appropriate information available to them.

Mitigation: This risk is mitigated. The goal of the NVC process is not to make an

Identifiable Information requires DHS personnel to apply the Fair Information Practice Principles to the collection, use, sharing, and maintenance of non-Privacy Act protected personally identifiable information; *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[32] For more information about the sharing with the NCTC, please *see* DHS/CBP/PIA-007(c) Electronic System for Travel Authorization (ESTA) (June 5, 2013), *available at* https://www.dhs.gov/privacy.

[33] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

[34] *See* https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

adjudication for CBP, but rather to provide a recommendation based on a consolidated view and analysis of the Vetting Support Responses and information made available by the ESTA Vetting Support Agencies. CBP Adjudicators will still conduct other appropriate vetting activities outside of the NVC process using ATS and other systems, ensuring the ESTA decision will be based on many factors not just the outcome of the NVC process.

CBP Adjudicators will also have access to NVC technology to view the Vetting Record, including the Vetting Support Responses, underlying information, and Analyst Notes before making the final decision on an ESTA application.

Uses of the Information

CBP will continue to use the information included in an individual's ESTA application to determine the eligibility of the foreign national to travel to the United States, including whether the visitor poses a law enforcement or security risk. With the addition of the vetting support provided through the NVC process, CBP will be better equipped to identify travelers of interest and distinguish them from legitimate travelers, thereby improving its security capabilities while also facilitating the entry of lawful visitors.

CBP will continue to vet the ESTA applicant information against selected security and law enforcement databases at DHS, including, but not limited to TECS and ATS, as well as against holdings from ESTA Vetting Support Agencies.

The addition of the NVC Analyst Recommendation to the ESTA Adjudicator only enhances CBP's ability to mitigate security gaps that may arise during the previous ESTA application process.

The sharing and use of information made available to CBP by the ESTA Vetting Support Agencies is governed by the information sharing agreements in place between those agencies, the classified NVC CONOP, and ESTA Vetting Support Agency guidelines and policies applicable to the sharing of intelligence, law enforcement, or other information. ESTA Vetting Support Agencies that are elements of the Intelligence Community must determine that sharing intelligence with CBP is permitted under their Attorney General Guidelines for the protection of U.S. person information, which are mandated by Executive Order 12333 and other applicable procedures, before they may provide it to CBP through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of ESTA data during the application process are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of the data are defined in publicly available documents such as the Privacy Notice (provided to ESTA applicant online), the ESTA and ATS SORNs, the ESTA PIA, and this PIA. These documents clearly outline that the information collected during the ESTA application process will be used to determine if an individual meets the requirements for eligibility for the ESTA program. It is also clear that the applicant's PII (and the U.S. point of contact PII required to be submitted with the ESTA application) will be used

for counterterrorism-related vetting.

Additionally, although the NVC process and technology will now be used, the scope of ESTA vetting against intelligence, law enforcement, and other information is not changing from what occurs today. That vetting will continue to be defined and governed by existing information sharing agreements between CBP and the ESTA Vetting Support Agencies, as well as the classified NVC CONOP. In the event of future proposals to modify the scope of ESTA vetting through the NVC, the Legal and PCRCL Working Groups will undertake a review of such proposals and advise the National Vetting Governance Board before it decides whether to approve any changes. This governance process helps to ensure that any changes to vetting activities occur in accordance with legal authorities and PCRCL protections.

Notice

Individuals who complete an ESTA application do so voluntarily and after having the opportunity to review the Privacy Notice, so it is expected they are fully aware they are submitting the information to CBP, the submission of the information is voluntary, how CBP intends to use that data, and the authorities under which it is collected. However, the ESTA application does require that the applicant provide a U.S. point of contact, specifically, a name, address, and telephone number. The U.S. point of contact may be an individual, a company, or another entity like a hotel where the individual plans to stay. If it is an individual, it may be a U.S. citizen or lawful permanent resident, who may not know that the ESTA applicant provided his or her information during the application process. The ESTA application also requires that the individual list the names, email addresses, and telephone numbers of both parents.

Privacy Risk: There is a risk that ESTA applicants and other individuals whose PII is included in an ESTA application (*e.g.*, U.S. point of contact) may not be aware and did not consent to their PII being used for vetting purposes.

Mitigation: Because the ESTA application process asks the applicant for information about individuals who may not be aware of the application or participate in its completion, this risk cannot be fully mitigated. There is no way for CBP to provide notice to these individuals because they are unlikely to be aware of or involved in the ESTA application itself. In lieu of this, DHS has taken a number of steps to provide general public notice of this fact, including publicly publishing this PIA and the ESTA PIA, planning to publish the unclassified version of the NVC Implementation Plan, and providing a Privacy Notice to the applicant at the time of application on the ESTA website.

If an individual who is not an ESTA applicant believes that DHS may have information about him or her as part of the ESTA application, he or she may seek to review this information by following the individual access, redress, and correction procedures described in the ESTA PIA.

Data Retention by the Project

Pursuant to the approved ESTA record retention schedule, ESTA application data is retained by CBP in the ESTA system for 15 years, the first three of which are in "active" status and the last 12 years in archive status. ESTA Vetting Records (which include collectively the Vetting Support

Request, Vetting Support Response, any Analyst Notes or Analyst Recommendation, and Adjudication) generated as part of the NVC process will be retained for the 15-year period as well. ESTA Vetting Support Requests sent to ESTA Vetting Support Agencies are retained for the periods of time provided in existing information sharing agreements, but those periods do not exceed the 15-year ESTA retention period unless the information is identified as retainable by the ESTA Vetting Support Agency in accordance with those agreements and its Attorney General Guidelines, in which case that individual record may be retained for a longer period in accordance with the information sharing agreement and the Vetting Support Agency's applicable records retention schedules and individual authorities to retain that information.

Privacy Risk: There is a risk that Vetting Records will be retained longer than necessary as a result of the NVC process and technology. Specifically, there is a risk that the Vetting Records created through this process and technology will be retained for longer than necessary.

Mitigation: This risk is mitigated. Unless the individual ESTA record is identified as permanently retainable by an ESTA Vetting Support Agency receiving the record in accordance with existing information sharing agreements, the retention period for the ESTA vetting record will not exceed 15 years at any point in the NVC process. If the record is found to be retainable in accordance with existing information sharing agreements, it may be retained for a longer period by that ESTA Vetting Support Agency, but only in accordance with that agency's legal authorities and other applicable policies and procedures, including, for those ESTA Vetting Support Agencies that are elements of the Intelligence Community, the standards for collecting and retaining foreign intelligence information described in the agency's Attorney General Guidelines for the protection of U.S. person information, which are required by Executive Order 12333.

Additionally, the existing ESTA information sharing agreements that CBP has with ESTA Vetting Support Agencies define how long those agencies may retain ESTA data and have been reviewed by oversight offices. For example, pursuant to the NCTC's memorandum of agreement with DHS, NCTC is allowed to temporarily retain ESTA records for up to two years in order to identify terrorism information, in support of its counterterrorism mission and in support of the mission of DHS. The two-year temporary retention period commences when DHS delivers the ESTA information to the NCTC. When the NCTC replicates ESTA information, the records will be marked with a "time-to-live" date, which will specify when the ESTA information will be deleted if it is not identified as terrorism information. The NCTC purges all ESTA records not determined to constitute terrorism information no later than two years from receipt of the record from DHS.

Information Sharing

Neither NSPM-9 nor the NVC provide any new legal authority to CBP or Vetting Support Agencies to collect, retain, store, or use ESTA information. All vetting activities for ESTA using the NVC process and technology are based on existing legal authorities. CBP will continue to share ESTA information in bulk with other federal counterterrorism partners (*e.g.*, NCTC). Existing external information sharing and access agreements supporting these vetting arrangements have been reviewed by CBP and the Vetting Support Agencies to ensure all legal, privacy, civil rights,

and civil liberties requirements are satisfied regarding the sharing and use of ESTA information in the NVC process. The classified NVC CONOP also contains provisions that govern the scope and protections of information sharing and use.

CBP has determined that disclosure of ESTA data to the Vetting Support Agencies to provide vetting support services is compatible with the purposes for which the data was collected and is authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3), specifically the routine uses set forth in the ESTA SORN (Routine Use G in this case). These information sharing agreements and the classified NVC CONOP have established the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy protections for the data.

Privacy Risk: There is a risk that the NVC process will result in information being shared with Vetting Support Agencies that do not have authority to support ESTA vetting activities or do not have data relevant to ESTA adjudications based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the PCRCL Working Group supporting the National Vetting Governance Board are charged with ensuring NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the NVC Implementation Plan and reviewed the NVC's technical designs, plans, and deployment to ensure they meet all legal and PCRCL requirements. These reviews included an evaluation by the working group members, which include representatives from various Vetting Support Agencies and DHS, to ensure that the vetting does not exceed the legal authorities of either CBP or the Vetting Support Agencies. In addition, agency legal counsel and PCRCL offices at CBP, DHS, and the Vetting Support Agencies are engaged in reviews of the same issues to ensure their agencies are complying with applicable laws and PCRCL policies, standards and practices.

Additionally, the existing information sharing agreements that CBP has with Vetting Support Agencies regarding the ESTA vetting program have been reviewed by oversight offices to ensure all legal and PCRCL requirements are being fulfilled.

Redress

During the process to incorporate ESTA into the NVC process, the existing ESTA redress process was reviewed within DHS and by the ESTA Vetting Support Agencies. A gap analysis was performed, and changes were made to redress procedures to ensure that redress would still occur in a timely and effective manner. These changes are expected to result in a more robust and independent review of the underlying information identified during the NVC process that may have led to the denial of an ESTA application.

In the event of an ESTA redress inquiry, CBP will follow all applicable redress procedures established by DHS's Traveler Redress Inquiry Program (DHS TRIP)[35] and the CBP Redress Office. They will facilitate the review and assessment of any information identified during the NVC process, including by coordinating with relevant ESTA Vetting Support Agency partners, as

[35] For more information about DHS TRIP, please *see* https://www.dhs.gov/dhs-trip.

appropriate, to ensure that the information used in the initial adjudication is still valid and determine if any updated information is available. CBP, in coordination with DHS TRIP, is developing written procedures for CBP personnel to follow when carrying out ESTA redress activities.

CBP and the ESTA Vetting Support Agencies will respond to requests for records in accordance with their applicable policies, practices, and procedures, including, but not limited to, responses to requests submitted by Congress, the Government Accountability Office, or members of the public under the Privacy Act, FOIA, or Judicial Redress Act. Any such requests to CBP for ESTA Vetting Support Agency responses provided in response to ESTA Vetting Support Requests will be coordinated with those agencies prior to response, and any request for ESTA data provided to an ESTA Vetting Support Agency as a Vetting Support Request will be coordinated by that agency with CBP prior to response. To the extent permissible under applicable law, the agency receiving the request will defer to the data originator for a determination as to the proper response. If non-attribution for a response provided by an ESTA Vetting Support Agency is, in that agency's conclusion, appropriate, CBP will respond to the request without attribution to the ESTA Vetting Support Agency, thereby protecting the source of the information from disclosure.

Privacy Risk: There is a risk that individuals will not have the ability to contest an ESTA adjudication that used information provided through the NVC process and technology as part of the determination.

Mitigation: This risk is mitigated. In addition to the DHS TRIP process described above, individuals who are denied an ESTA travel authorization may still apply for a visa through the normal process of the Department of State, where an extensive review of applicant identity and vetting information occurs.[36]

Auditing and Accountability

The NVC process and technology includes an audit function that captures electronic messages and transactions within its own technology and with other systems involved in the ESTA vetting workflow. It has the capability to fully review the actions that occurred in the workflow, beginning with the original Vetting Support Request, through all ESTA Vetting Support Responses, to any Analyst Recommendations. The format and location of these records permits the reporting of metrics, support of redress processes, and retrieval records for compliance and oversight purposes.

Responsible Officials

Monte Hawkins
Director
National Vetting Center
Department of Homeland Security

[36] Federal law and regulation do not permit an appeal for an ESTA denial or revocation. *See* 8 U.S.C. § 1187(h)(3)(C)(4); 8 CFR 217(g).

Approval Signature

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

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

NVC PIA Addendum 2:

Vetting in Support of Enduring Welcome (EW)

Last updated October 23, 2023 (back to top)

On August 29, 2021, President Biden directed the Department of Homeland Security (DHS) to lead the implementation of ongoing efforts across the federal government to support vulnerable individuals in Afghanistan, including those who worked alongside U.S. personnel during the past two decades, as they safely resettle in the United States. These coordinated efforts were known as Operation Allies Welcome (OAW) and continue today through the Enduring Welcome (EW) initiative.

EW Initial Parole Process

EW-covered individuals were screened and vetted by the U.S. government prior to their arrival in the United States, with the parallel goals of protecting national security and protecting these vulnerable Afghan evacuees. After initial vetting overseas, individuals who presented themselves as covered by EW at a port of entry were inspected by U.S. Customs and Border Protection (CBP). On a case-by-case basis, CBP paroled,[37] for humanitarian reasons, EW-covered individuals for a period of up to two years.

EW parolees were subject to additional security vetting to supplement their initial overseas vetting with more fulsome information and continue to be subject to additional recurrent vetting for the duration of their parole. In October 2021, the National Vetting Center (NVC) began to support this vetting through its process and technology by facilitating the submission of EW Vetting Support Requests to Vetting Support Agencies (VSA). Additionally, all EW Vetting Support Requests were provided separately to the National Counterterrorism Center (NCTC) for the limited purpose of enabling the NCTC to provide continuous vetting support for the EW parolees, thereby helping to ensure that the U.S. government is aware of any EW parolees identified as posing a threat to national security or public safety through information obtained subsequent to their parole.

As part of NVC's initial support to EW, when an EW Vetting Support Agency matched information in a Vetting Support Request to derogatory information, the match was provided to U.S. Immigration and Customs Enforcement (ICE) Vetting Analysts for review. ICE Vetting Analysts, in coordination with other interagency partners, as appropriate, would then analyze the information provided by EW Vetting Support Agencies and make a recommendation on whether to refer an EW parolee for additional investigation, which may have ultimately resulted in a determination that termination of parole was warranted under 8 C.F.R. § 212.5, on a case-by-case

[37] Parole allows an individual, who may be inadmissible or otherwise ineligible for admission into the United States, to be paroled into the United States for a temporary period. The Immigration and Nationality Act (INA) allows authorized DHS officials to use their discretion to parole any alien applying for admission into the United States temporarily for urgent humanitarian reasons or significant public benefit. (*See* 8 U.S.C. § 1182(d)(5); 8 C.F.R. § 212.5). An individual who is paroled into the United States has not been formally admitted into the United States for purposes of immigration law but is lawfully present during the parole period.

basis.[38]

EW Re-Parole and Extension of Parole Process

On June 8, 2023, DHS announced a new process that will enable EW parolees to request a continuation of their parole and their ability to live and work legally in the United States. This streamlined process will generally provide for an additional two-year period of parole for EW-covered individuals who are granted re-parole or extension of parole. This action is part of the Department's ongoing commitment to provide robust, fair, and equitable screening and vetting that protects national security; public safety; and the safety, security, and well-being of the thousands of Afghan nationals who arrived in the United States through EW. Accordingly, the National Vetting Governance Board (NVGB) recognizes the need to continue to provide NVC support to the EW parolee program by facilitating the delivery of Vetting Support Requests to appropriate Vetting Support Agencies for re-parole purposes. The NVC will also continue to provide EW Vetting Support Requests to the NCTC for continuous vetting support.

Moving forward, unlike the initial parole process, U.S. Citizenship and Immigration Services (USCIS) will serve as the sole adjudicating agency for EW parole, re-parole, and extension of parole. In this capacity, USCIS will review all NVC matches to derogatory information for this population, whether they are the result of:

- Recurrent vetting associated with the initial CBP parole at a port of entry or a new Vetting Support Request based on obtaining new biographic information subsequent to initial CBP parole at a port of entry,[39]
- A new Vetting Support Request based on a request for re-parole (filing an I-131),
- A new Vetting Support Request in support of Agency action to extend parole for individuals with a pending I-485 and/or I-589,
- Or recurrent vetting associated with the USCIS re-parole or extension of parole.

This Privacy Impact Assessment (PIA) Addendum updates and replaces the prior Privacy Impact Assessment Addendum for vetting in support of the EW parolee program.

NVC Support to EW Parole Program

EW parolees between the ages of 14 and 79 will be vetted through the NVC process and technology. The starting point for EW re-parole vetting through the NVC is the transmission of a Vetting Support Request, which consists of EW parolee biographic information, to the EW Vetting Support Agencies. The EW Re-Parole Vetting Support Request is comprised of the parolee's initial Operation Allies Welcome selectors combined with new selectors from one of the following three

[38] For more information on the previous ICE adjudication process, *see* DHS/ICE/PIA-049 ICE Parole and Law Enforcement Programs Unit Case Management System, *available at* https://www.dhs.gov/privacy.
[39] However, if an individual is still in valid parole status pursuant to their initial CBP parole, USCIS will refer the derogatory information to CBP to consider whether to terminate the individual's parole. It is long-standing Agency practice that ICE, CBP, and USCIS do not terminate parole that was granted by one of the other agencies.

data sources:

- USCIS Form I-131, *Application for Travel Document*, which the parolee must file to request re-parole if they have not filed an application for asylum (I-589) or adjustment of status (I-485) with USCIS;
- USCIS Form I-485, *Application to Register Permanent Residence or Adjust Status*, if the parolee has a pending adjustment filing with USCIS; or
- USCIS Form I-589, *Application for Asylum and for Withholding of Removal*, if the parolee has a pending asylum filing with USCIS.[40]

USCIS Vetting Analysts then use the NVC technology to receive and review any relevant and appropriate classified or unclassified records made available by one or more Vetting Support Agencies. USCIS Vetting Analysts review the information and produce a "summary"[41] containing an analysis of relevant findings that is provided to a USCIS immigration benefit adjudicator. The USCIS adjudicator will then decide whether to grant the applicant(s) re-parole pursuant to 8 C.F.R. § 212.5 or extend their existing parole for two years.

The NVC's process and technology will allow for the:

- Distribution of Vetting Support Requests to EW Vetting Support Agencies;
- Receipt of Vetting Support Responses from EW Vetting Support Agencies and distribution to USCIS;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for USCIS Vetting Analysts to access classified and unclassified records identified by an EW Vetting Support Agency as relevant to a Vetting Support Request;
- Support for USCIS Vetting Analysts to document their analysis and summaries;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Managing access to data by individual users and infrastructure according to pre-determined rules and standards;

[40] Parolees who have a pending I-485 or I-589 application with USCIS and whose initial parole and employment authorization expires in 2023 or 2024 are being granted an extension to their initial parole (rather than re-parole), pending the screening and vetting process, and do not have to apply for re-parole with USCIS. For vetting purposes, however, there is no distinction made between Re-parole Vetting Support Requests and Extension of Parole Vetting Support Requests.

[41] The classified records made available by one or more Vetting Support Agencies will not be directly accessible by USCIS benefit adjudicators. Most of the USCIS personnel who will directly access these classified records in the near term are neither trained benefits adjudicators nor are they authorized by USCIS to adjudicate benefit requests. Instead, their role is to access, review, analyze, and synthesize the classified records to make summaries available to USCIS' adjudicative personnel.

- Managing the retention of data according to approved record schedules and information sharing agreements;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for parolee redress processes, FOIA requests, discovery in litigation, and other data retrieval requirements.

As it relates to handling recurrent vetting matches for initial EW parole requests, EW parole information is derived from USCIS Form I-765, *Application for Employment Authorization*, if submitted by the parolee, and certain information accessible through CBP's Automated Targeting System (ATS).[42] Information contained within the Vetting Support Request is limited to that of the EW parolee and does not include information concerning U.S. citizens or lawful permanent residents (U.S. persons). Initial EW Vetting Support Requests may have also been enhanced with additional information relating to the subjects of EW Vetting Support Requests using a CBP-developed capability, known as Unified Person for Vetting (UPV). Unified Person for Vetting correlates data provided by individuals in the context of EW against related, authoritative data sources already available within CBP's Automated Targeting System and enhances the Vetting Support Requests with additional biographic information from those data sources where a match is identified. This process provides additional information for Vetting Support Agencies to match against and allows USCIS to make better informed decisions based on all relevant and appropriate information available to it. Accordingly, when the NCTC matches information in a Vetting Support Request to derogatory information during recurrent vetting, the match will be provided to USCIS Vetting Analysts for review and USCIS adjudicators will determine whether termination of parole is warranted under 8 C.F.R. § 212.5, on a case-by-case basis.

Additionally, the CBP National Targeting Center (NTC) is leveraging existing capabilities and system processes to support USCIS' and ICE's efforts related to the EW population. CBP's ongoing unclassified vetting efforts are intended to compliment and inform DHS's administration of immigration benefits and immigration enforcement. A limited number of CBP/NTC analysts have been approved access to classified EW vetting results to support these efforts.

Privacy Impact Analysis

Authorities and Other Requirements

- The information requested on the I-131 application, and the associated evidence, is collected by USCIS under the Immigration and Nationality Act (INA) sections 103, 208(c)(1)(C), 211, 212(d)(5)(A), and 215 and 8 C.F.R. §§ 211.1(a)(3-4), 212.5, and 223.1-223.3.
- The information requested on the I-485 application, and the associated evidence, is collected by USCIS under INA sections 101 et seq., as amended, and related public laws and regulations.
- The information requested on the I-589 application, and the associated evidence, is collected by USCIS under INA sections 208 and 241(b)(3).
- The information requested on the I-765 application, and the associated evidence, is

collected by USCIS under the INA, 8 U.S.C. § 1324a, 8 C.F.R. § 274a.12, and 8

[42] See DHS/CBP/PIA-006 Automated Targeting System (ATS) and subsequent updates, available at https://www.dhs.gov/privacy.

C.F.R. § 274a.13.

- USCIS' authority to perform screening and vetting on applicants for immigration benefits, including through use of information received from other agencies, derives from 8 U.S.C. §1105(a).
- CBP's Automated Targeting System derives its authority primarily from 8 U.S.C. § 1357; 19 U.S.C. §§ 482, 1461, 1496, and 1581-82; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). Other relevant authorities concerning these activities include 6 U.S.C. §§ 111 and 211; 8 U.S.C. §§ 1103, 1182, 1225- 25a, and 1324; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623-24, and 1644-44a.

The use of the NVC process and technology for the EW parole program does not provide any new legal authorities to USCIS and CBP to collect, retain, store, or use information, or to make adjudications based on vetting. All activities undertaken through the NVC process are based on USCIS' and CBP's existing legal authorities. EW Vetting Support Agencies similarly are engaged in the vetting process pursuant to their existing legal authorities.

System of Records Notice (SORN) coverage for EW parole program activities is provided by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records;[43] DHS/USCIS-007 Benefits Information System;[44] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records;[45] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records;[46] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records;[47] and DHS/CBP-006 Automated Targeting System.[48]

[43] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[44] DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019).
[45] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015).
[46] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (October 19, 2016).
[47] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018).
[48] DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012).

Characterization of the Information

To apply for a continuation of their parole after the expiration of the initial parole period, EW parolees are required to file a USCIS Form I-131, unless they have filed an I-485 and/or I-589 that remains pending before USCIS. The biographic data collected on these forms will be used to generate Vetting Support Requests. If derogatory information is found during the NVC process, USCIS Vetting Analysts will analyze the information provided by EW Vetting Support Agencies and provide a summary to USCIS adjudicators so the adjudicators may determine whether to grant re-parole or an extension of their existing parole.

For recurrent vetting associated with initial parole requests, EW parolees may have chosen to file Form I-765 to request employment authorization and an Employment Authorization Document (EAD). This form collected various biographic data elements that were used as part of the initial Vetting Support Request, if available. In addition, the Vetting Support Request may have contained certain information on EW parolees that was maintained in or accessible through CBP's Automated Targeting System. This may include information that was supplied by EW parolees overseas before arriving in the United States, information that was collected by DHS personnel at ports of entry, information that was supplied by EW parolees to DHS in the United States, and Unified Person for Vetting information correlated from CBP's Automated Targeting System.

If the NCTC matches information in a Vetting Support Request to derogatory information during recurrent vetting, the match will be provided to USCIS Vetting Analysts for review and USCIS adjudicators will determine whether termination of parole is warranted under 8 C.F.R. § 212.5, on a case-by-case basis.

The following personally identifiable information (PII) may be included in Vetting Support Requests for continuous vetting associated with initial parole or extension of initial parole:

- A-Number
- Fingerprint Identification Number
- Full Name
- Aliases
- Date of Birth
- Country of Birth
- Country of Citizenship
- Gender
- Physical Address
- Mailing Address
- Phone Number

- Email Address
- Social Security Number
- Passport Number

The following personally identifiable information may be included in Vetting Support Requests for re-parole:

- A-Number
- Fingerprint Identification Number
- Full Name
- Aliases
- Date of Birth
- Country of Birth
- Country of Citizenship
- Gender
- Physical Address
- Mailing Address
- Phone Number
- Email Address
- Social Security Number
- Receipt Number

The following personally identifiable information may be included in Vetting Support Requests for instances when additional information is supplied to DHS by EW parolees once already paroled into the United States:

- A-Number
- I-94 Number[49]
- Name
- Address

[49] DHS issues Form I-94, Arrival/Departure Record, to noncitizens who are admitted to the United States, adjusting status while in the United States, or extending their stay. All persons need a Form I-94 except U.S. citizens, returning resident noncitizens, noncitizens with immigrant visas, and most Canadian citizens visiting or in transit. Air and sea travelers will be issued I-94s during the admission process at the port of entry.

- Aliases
- Date of Birth
- Country of Birth
- Country of Citizenship
- National Identity Number
- Current primary phone number and those used in the past five years
- Current secondary phone number
- Current cellular phone number
- Addresses during the past five years
- Email addresses used in the last five years
- Passport Number and Country of Issuance
- Name, phone number, email address, and physical address of Person of Contact in the United States
- Receipt Number (If known)

Privacy Risk: There is a risk that USCIS may make decisions to extend parole, grant re-parole, not grant re-parole, decline to extend parole, or terminate an individual's parole status based on inaccurate information identified during the NVC process.

Mitigation: This risk is partially mitigated. Most of the information used to conduct vetting is collected directly from EW parolees, which should help ensure data accuracy upon collection. However, if an EW parolee provides inaccurate information, it may result in inaccurate results from the NVC process. Further, as it relates to recurrent vetting for initial parole, some Unified Person for Vetting information correlated from CBP's Automated Targeting System may come from other government data sources; CBP relies on those source systems and their data collection processes to ensure that data maintained in or ingested by CBP's Automated Targeting System is accurate and complete. EW Vetting Support Agencies are required to apply their analytic standards to ensure that information regarding the EW parolee is objective, timely, relevant, and accurate. For example, EW Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive 203, which requires that personally identifiable information is disseminated "only as it relates to a specific analytic purpose . . . [and] consistent with [Intelligence Community] element mission and in compliance with [Intelligence Community] element regulation and policy, including procedures to prevent, identify, and correct errors in [personally identifiable information]."[50] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any

[50] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

factors affecting source quality and credibility.[51]

The summary provided by the USCIS Vetting Analysts inform adjudicative decision-making, but do not determine the ultimate decision regarding parole status. It is the responsibility of USCIS Adjudicators to evaluate the substance and assessed reliability of the additional information provided by the EW Vetting Support Agencies, in conjunction with other information available to USCIS, in making case-by-case determinations on an individual's parole status.

Privacy Risk: There is a risk that USCIS will make adjudications based solely on the Analyst summary and not all the appropriate information available to them.

Mitigation: This risk is mitigated. The goal of the NVC process is not to make an adjudication for USCIS, but rather to facilitate a summary to USCIS adjudicators based on a consolidated view and analysis of the Vetting Support Responses and information made available by the EW Vetting Support Agencies. The USCIS adjudicator will then make a decision based on the totality of the information available to them, such as information in the application and supporting documentation as well as the results of other USCIS security checks. USCIS will also have access to NVC technology to view the Vetting Record, including the Vetting Support Responses, underlying information, and Analyst Notes before deciding to re-parole, extend, or terminate EW parole or take no further action.

Uses of the Information

USCIS will use the information collected from EW parolees to analyze potential threats to national security and determine whether the information available raises a question as to whether urgent humanitarian reasons and significant public benefit warrant the continued presence of the parolee in the United States, in the exercise of discretion. With the additional vetting support provided through the NVC process, USCIS will be better equipped to identify individuals who may pose a security risk. NVC vetting support will improve U.S. government security capabilities while also facilitating the resettlement of EW parolees for humanitarian purposes.

The sharing and use of information made available to USCIS by the EW Vetting Support Agencies is governed by the information sharing agreements in place between those agencies; EW Vetting Support Agency guidelines; and policies applicable to the sharing of intelligence, law enforcement, or other information. EW Vetting Support Agencies that are elements of the Intelligence Community must determine that sharing intelligence with USCIS is permitted under their Attorney General Guidelines which are mandated by Executive Order 12333 and other applicable procedures, before they may provide the intelligence to USCIS through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of EW parolee's

[51] *See* https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

data are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of the data are defined in publicly available documents such as this Privacy Impact Assessment, other relevant Privacy Impact Assessments, and System of Records Notices covering the collection of the USCIS I-131 information,[52,53] USCIS I-765 information,[54,55] USCIS I-485 information,[56,57] USCIS I-589 information,[58,59] and the CBP Automated Targeting System Privacy Impact Assessment and System of Records Notice.[60,61] These documents clearly outline the information collected and explain that the information may be shared with other federal departments and agencies for the purpose of screening and vetting.

Although the NVC process and technology will now be used, the scope of EW vetting against intelligence, law enforcement, and other information is not changing from the manual process that occurred previously. Vetting will continue to be defined and governed by existing information sharing agreements and arrangements between USCIS, CBP, and the EW Vetting Support Agencies.

Notice

Individuals who complete and file an I-131, I-485, I-589, and/or I-765 application do so voluntarily after having the opportunity to review the Privacy Notice. It clearly states the authority for the collection of information, that applicants are submitting to DHS/USCIS, that the submission of the information is voluntary, and how that data will be used by DHS/USCIS.

---

[52] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System and Associated Systems and DHS/USCIS/PIA-051 Case and Activity Management for International Operations, *available at*: www.dhs.gov/privacy.
[53] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System 82 FR 43556 (September 18, 2017); DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019); and DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36950 (July 31, 2018).
[54] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems; DHS/USCIS/PIA-056 USCIS ELIS; DHS/USCIS/PIA-061 Benefit Request Intake Process; and DHS/USCIS/PIA-071 myUSCIS Account Experience, *available at* www.dhs.gov/privacy.
[55] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017); DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019); DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015); DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (October 19, 2016).
[56] DHS/USCIS/PIA-051 Case and Activity Management for International Operations, *available at*: www.dhs.gov/privacy.
[57] DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019); DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017).
[58] *See* DHS/USCIS/PIA-027(d) USCIS Asylum Division and DHS/USCIS/PIA-051 Case and Activity Management for International Operations, *available at*: www.dhs.gov/privacy.
[59] DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017); DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (November 30, 2015).
[60] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[61] DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012).

Most of the information regarding EW parolees within CBP's Automated Targeting System is collected directly from the parolees. Additional information regarding EW parolees within CBP's Automated Targeting System may be derived from other government data sources. Notice for this additional information is provided through the applicable source System of Records Notices and Privacy Impact Assessments (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information.

Additional information supplied by EW parolees is supplied on a consensual basis, consistent with the conditions of parole.

Privacy Risk: There is a risk that EW parolees may not be aware and did not consent to their personally identifiable information being used for vetting purposes.

Mitigation: This risk is partially mitigated. Individuals completing and submitting the I-131, I-485, I-589, and/or I-765 are required to authorize the release of information contained in the application, supporting documents, and their USCIS records to other entities and persons where necessary for the administration and enforcement of U.S. immigration law. However, as it relates to recurrent vetting, certain information stored in CBP's Automated Targeting System is not directly collected from the EW parolee. Information within CBP's Automated Targeting System is provided by various government data sources, and notice is provided through the applicable source System of Records Notices and Privacy Impact Assessments (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information. Certain supplemental information supplied by EW parolees is provided on a consensual basis, consistent with the conditions of parole.

Data Retention by the Project

The NVC will retain EW Vetting Records, which include the Vetting Support Request, Vetting Support Response, Analyst Notes (if applicable), Analyst Summaries, and Adjudication for a period of two years, which parallels the two-year parole period granted to many individuals under EW.

EW Vetting Support Agencies are separately authorized to temporarily maintain EW Vetting Records outside the NVC process and technology for up to two years from the time of receipt for the limited purpose of providing recurrent vetting support, as permitted by their respective legal authorities, unless identified as retainable by an EW Vetting Support Agency in accordance with its Attorney General Guidelines or identified by a law enforcement agency or administrative agency as retainable in a Privacy Act compliant system. In such cases, a record may be retained for a longer period in accordance with the applicable records retention schedules and individual authorities to retain the information.

Privacy Risk: There is a risk that Vetting Records created through the NVC process and technology will be retained longer than necessary.

Mitigation: For Vetting Records maintained within DHS systems using the NVC process and technology, this risk is mitigated. The NVC will tag EW Vetting Records to ensure that

information is not retained for longer than two years. Additionally, the retention period for the vetting support records applicable to each vetting program is documented internally in classified documents that outline the specific processes for those particular vetting programs. This documentation defines the authorized retention period of Vetting Support Requests shared with EW Vetting Support Agencies and the purposes for such sharing. Vetting Support Agencies may retain vetting records for longer periods when, for example, they are identified as foreign intelligence or are relevant to law enforcement investigations, in accordance with existing information sharing agreements, applicable law, and policy.

For Vetting Support Request information ingested by EW Vetting Support Agencies' internal systems, this risk is not fully mitigated solely by NVC technologies. This risk is instead further mitigated by the internal retention controls of the Vetting Support Agencies, including records retention schedules, the National Security Act, and Executive Order 12333-derived retention limitations.

Privacy Risk: There is a risk that some individuals may gain U.S. Person status during this period and are not removed from recurrent vetting in a timely manner.

Mitigation: The risk is partially mitigated. Upon discovery of status change during a Vetting Support Agency analyst's manual review, the identified record is then handled in accordance with the Vetting Support Agency's Executive Order 12333 Attorney General Guidelines. Additionally, USCIS will identify U.S. Person status changes on a weekly basis for EW parolees that are in the recurrent vetting process and the NVC will inform the NCTC of these status changes so that they may be handled in accordance with their Executive Order 12333 Attorney General Guidelines.

Information Sharing

Neither National Security Presidential Memorandum (NSPM)-9 nor the NVC provide any new legal authority to USCIS, CBP, or EW Vetting Support Agencies to collect, retain, store, or use information as part of the EW mission. All vetting activities for EW using the NVC process and technology are based on existing legal authorities. Existing external information sharing and access agreements supporting these vetting arrangements have been reviewed by USCIS, CBP, and the Vetting Support Agencies to ensure all legal, privacy, civil rights, and civil liberties requirements are satisfied regarding the sharing and use of EW information in the NVC process. These information sharing agreements and the classified EW Addendum to the NVC-Intelligence Community Support Element Concept of Operations have established the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy, civil rights, and civil liberties protections for the data.

USCIS and CBP have determined that disclosure of their EW parolee data to the Vetting Support Agencies to provide vetting support services is compatible with the purposes for which the data was collected and is authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3) (specifically, the routine uses set forth in the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records (especially Routine Uses G and EE)); DHS/USCIS-007 Benefits Information System (especially Routine Uses G, K, and W); DHS/USCIS-010 Asylum

Information and Pre-Screening System of Records (especially Routine Uses G, H, and I); DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records (especially Routine Uses G and I); DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records (especially Routine Uses H, I, and R); and DHS/CBP-006 Automated Targeting System (especially Routine Uses G and H).

Privacy Risk: There is a risk that the NVC process will result in information being shared with Vetting Support Agencies that do not have authority to support EW vetting activities or do not have data relevant to EW adjudications based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the Privacy, Civil Rights and Civil Liberties (PCRCL) Working Group supporting the National Vetting Governance Board are charged with ensuring NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the NVC Implementation Plan, the classified EW Addendum to the NVC-Intelligence Community Support Element Concept of Operations, and the NVC's technical designs, plans, and deployment to ensure they meet all legal and privacy, civil rights, and civil liberties requirements. These reviews included an evaluation by the working group members, which include representatives from various Vetting Support Agencies and DHS, to ensure that the vetting does not exceed the legal authorities of either DHS or the Vetting Support Agencies. In addition, agency legal counsel and privacy, civil rights, and civil liberties offices at DHS and the Vetting Support Agencies are engaged in reviews of the same issues to ensure their agencies are complying with applicable laws and privacy, civil rights, and civil liberties policies, standards, and practices. Information sharing agreements are in place to facilitate information sharing between USCIS, CBP, and EW Vetting Support Agencies. These agreements have also been reviewed by oversight offices to ensure that all legal and privacy, civil rights, and civil liberties requirements are being fulfilled.

Redress

The NVC does not possess the authority to collect, retain, use, or share information of its own and therefore does not provide any specific redress process. The NVC defers to the process or processes that Adjudicating Agencies employ to provide redress to individuals regarding their adjudications, where applicable.

If EW vetting results are considered in connection to a case-by-case determination that results in the termination of parole, non-citizens will receive all process due under the Immigration and Nationality Act.

USCIS and the EW Vetting Support Agencies will respond to requests for records in accordance with their applicable policies, practices, and procedures, including, but not limited to, responses to requests submitted by Congress, the Government Accountability Office, or members of the public under the Privacy Act, Freedom of Information Act, or Judicial Redress Act. Any such requests to USCIS for EW Vetting Support Agency responses provided in response to Vetting Support Requests will be coordinated with those agencies prior to response, and any request

for EW data provided to an EW Vetting Support Agency as a Vetting Support Request will be coordinated by that agency with USCIS prior to response. To the extent permissible under applicable law, the agency receiving the request will defer to the data originator for a determination as to the proper response. If non-attribution for a response provided by an EW Vetting Support Agency is, in that agency's conclusion, appropriate, USCIS will respond to the request without attribution to the EW Vetting Support Agency, thereby protecting the source of the information from disclosure.

Privacy Risk: There is a risk that individuals will not have the ability to contest an EW parole termination that used information provided through the NVC process and technology as part of the determination.

Mitigation: This risk is partially mitigated. If vetting results are considered in a determination that parole will not be extended, re-parole will not be granted, or results in the termination of EW parole and initiation of removal proceedings, EW parolees will receive all process due under the Immigration and Nationality Act. Further, individuals seeking notification of and access to any records related to USCIS' parole adjudication may submit a request in writing to the USCIS Freedom of Information Act (FOIA) Officer by following the instructions at: https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act. Meanwhile, individuals seeking notification of and access to any records related to ICE's previous parole adjudications may submit a request in writing to:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act or the Freedom of Information Act (for those individuals who are not U.S. citizens or lawful permanent residents and whose records are not covered by the Judicial Redress Act) to prevent harm to law enforcement investigations or national security interests.

Auditing and Accountability

The NVC process and technology includes an audit function that captures electronic messages and transactions within its own technology and with other systems involved in the EW vetting workflow. It has the capability to allow full review of the actions that occurred in the workflow, beginning with the original Vetting Support Request, through all EW Vetting Support Responses, to any analyst summaries. The format and location of these records permits the reporting of metrics, support of redress processes, and retrieval of records for compliance and oversight purposes.

Responsible Officials

Andrew Douglas
Director (Acting)
National Vetting Center
Department of Homeland Security

Approval Signature

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

_____

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

NVC PIA Addendum 3:

United States Refugee Admissions Program (USRAP)

Last updated March 22, 2022 (back to top)

USRAP Background

The United States Refugee Admissions Program (USRAP) processes qualified refugees for resettlement into the United States under section 207 of the Immigration and Nationality Act (INA) (codified at 8 U.S.C. § 1157). It is an interagency effort involving several U.S. government agencies. The Bureau of Population, Refugees, and Migration (PRM) at the Department of State (State) has overall USRAP management responsibility outside the United States and program oversight. The Bureau of Population, Refugees, and Migration manages Resettlement Support Centers (RSC) through memoranda with international organizations and cooperative agreements with non-governmental organizations. Cases are typically referred to the USRAP by the United Nations High Commissioner for Refugees (UNHCR) or by U.S. Embassies and consulates. Additionally, certain groups of individuals may be designated by the U.S. government as eligible to self-apply for resettlement directly under the USRAP.

DHS's U.S. Citizenship and Immigration Services (USCIS) has been delegated the responsibility for adjudicating applications and reviewing case decisions, and U.S. Customs and Border Protection (CBP) is responsible for determining admissibility at ports of entry and admitting eligible applicants as refugees into the United States. The USRAP vetting process is supported by various intelligence community partners, State (through the Bureau of Population, Refugees, and Migration), and DHS (through USCIS and CBP). To be eligible, refugee applicants must meet the INA definition of a refugee,[62] not be firmly resettled in another country, otherwise be admissible, and merit a favorable exercise of discretion as determined by USCIS.

Bureau of Population, Refugees, and Migration -funded Resettlement Support Centers[63] receive applications for those who are referred by the UNHCR, or other agency, for consideration for resettlement into the United States or who are otherwise eligible to apply for resettlement into the United States under the USRAP. Under program requirements, Resettlement Support Centers collect information from the applicants, including biographic data on the principal applicant, any derivative applicants (i.e., a spouse and any unmarried children under the age of 21 who are seeking

[62] Section 101(a)(42) of the INA (codified at 8 U.S.C. § 1101(a)(42)) defines a refugee as "any person who is outside any country of such person's nationality or, in the case of a person having no nationality, is outside any country in which such person has habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself to the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion."

[63] Resettlement Support Centers are international and nongovernmental organizations that carry out administrative and processing functions for the USRAP under cooperative agreements or memoranda with State. The Bureau of Population, Refugees, and Migration funds Resettlement Support Centers in Vienna, Austria; Istanbul, Turkey; Amman, Jordan; Nairobi, Kenya; Kyiv, Ukraine; Bangkok, Thailand; and San Salvador, El Salvador. Some of these Resettlement Support Centers have smaller sub-offices in additional processing locations.

to resettle with the principal applicant), and any other immediate family members[64] to prepare cases for security screening, interviews, adjudication by USCIS, and potential resettlement to the United States. The biographic information collected from the applicant, derivative applicants, and immediate family members are then provided to State's refugee case management system, and ultimately to USCIS to initiate a vetting request with its vetting partners.

The INA sets forth numerous categories of inadmissibility for individuals seeking admission to the United States, including a series of categories pertaining to criminal and related grounds and a separate series pertaining to security and related grounds, which includes grounds pertaining to terrorist activities. To ensure the enforcement of these provisions, the INA separately authorizes State and DHS to maintain direct and continuous relationships with intelligence and law enforcement agencies within the U.S. government. For decades, State and DHS have leveraged this authority to support the review of refugee cases to identify applicants that may fall within one or more of the security-related categories of inadmissibility in the INA or other relevant provisions of U.S. law or policy.

Once the vetting partners communicate their results to USCIS, and it is determined that the applicant is eligible for resettlement (including that all required security checks have been resolved), the Resettlement Support Center conducts necessary out-processing steps (a medical exam, cultural orientation, a sponsorship agreement with a domestic resettlement agency, etc.) and refers the case to the International Organization for Migration, an inter-governmental organization that assists in arranging refugee travel to the United States.

As with all individuals seeking admission to the United States at a port of entry, CBP inspects the applicant and determines whether the applicant is admissible. CBP vets the refugee traveler prior to boarding, conducts an inspection upon arrival at the U.S. port of entry, and admits eligible applicants into the country as refugees. The Office of Refugee Resettlement at the Department of Health and Human Services and various non-governmental organizations provide resettlement benefits and assistance services to admitted refugees once they have arrived.

National Vetting Center (NVC) Support to USRAP Vetting

The NVC leverages the process and technology described in the NVC Privacy Impact Assessment above to facilitate the vetting of refugee application data, helping to ensure that adjudications are informed by all appropriate responsive information held by USRAP Vetting Support Agencies in a timely and comprehensive manner while also safeguarding sensitive data included in and related to applications for refugee resettlement. As explained in the Privacy Impact Assessment, the NVC does not make recommendations or adjudications. Its role is limited to that of a facilitator or service provider of the NVC process and technology used to facilitate vetting and adjudications by USCIS.

The starting point for the vetting of all refugee applicants through the NVC process and technology is the transmission of a Vetting Support Request, which includes refugee application

[64] This generally includes parents, siblings, and any spouse or children, even if they are not included on the application for resettlement.

data, to the USRAP Vetting Support Agencies. Existing memoranda of agreement between State, USCIS, and the Vetting Support Agencies determine which data fields in the application are included in the Vetting Support Request and how they are delivered to each Vetting Support Agency. USCIS Vetting Analysts then use the NVC technology to receive and review any relevant and appropriate classified or unclassified record made available by one or more Vetting Support Agencies. USCIS Vetting Analysts review the information and make a recommendation as to whether the applicant(s) may pose a national security, fraud, or public safety concern. This recommendation is communicated to a USCIS Refugee Officer, who reviews the recommendation along with all other information available to them to decide whether to approve or deny the application for refugee resettlement.

The NVC's process and technology will allow for:

- Distribution of Vetting Support Requests (*i.e.*, data from USRAP applications) to Vetting Support Agencies;
- Receipt and distribution of Vetting Support Responses from Vetting Support Agencies to USCIS;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for USCIS Vetting Analysts to access classified and unclassified information identified by Vetting Support Agencies as relevant to a Vetting Support Request;
- Support for USCIS Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Managing access to and handling of data by individual users and infrastructure according to pre-determined rules and standards;
- Managing the retention of data according to approved State/USCIS record schedules and information sharing agreements;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for redress procedures (where applicable), FOIA requests, discovery in litigation, and other data retrieval requirements.

Privacy Impact Analysis

Authorities and Other Requirements

The USRAP processes qualified refugees for resettlement into the United States under section 207 of the INA.[65] The use of the NVC process for this vetting program does not require any new legal authorities to collect, retain, store, or use information, or to make adjudications based on vetting. All activities undertaken through the NVC process are based on CBP's, USCIS's, and State's existing legal authorities. USRAP Vetting Support Agencies similarly are engaged in the vetting process pursuant to their own existing legal authorities.

[65] 8 U.S.C. § 1157.

USRAP records are maintained in various State and DHS systems and are subject to several System of Records Notices (SORN). The System of Records Notice coverage includes but is not limited to the applications; related forms; internal correspondence and notes relating to USRAP adjudications; and information regarding applicants' family members, and employers (potentially including U.S. citizens and lawful permanent residents (U.S. persons)).

The refugee application, supplemental evidence, and supporting documentation are maintained in State's refugee case management system, which is governed by State's Refugee Case Records System of Records Notice (STATE-59);[66] in the applicant's USCIS A-File, which is governed by the A-File System of Records Notice (DHS/USCIS/ICE/CBP-001);[67] and in USCIS systems governed by the Refugee Access Verification Unit System of Records Notice (DHS/USCIS-008).[68] The Immigration Biometric and Background Check System of Records Notice (DHS/USCIS-018)[69] and the Refugee Case Processing and Security Screening System of Records Notice (DHS/USCIS-017)[70] govern the information collected, used, and maintained as part of the adjudication process, including decisional information. Finally, USCIS's Fraud Detection and National Security (FDNS) Directorate may review certain applications or individuals for potential fraud, public safety, and national security concerns. The Fraud Detection and National Security System of Records Notice (DHS/USCIS-006)[71] governs how Fraud Detection and National Security creates and uses information during those reviews.

Characterization of the Information

State and USCIS will continue to collect and use the same information collected from individuals throughout the application process for refugee resettlement, and USCIS Refugee Officers will continue to receive recommendations from USCIS Vetting Analysts. These recommendations are generated by USCIS Vetting Analysts who, acting under USCIS authorities, analyze information made available by Vetting Support Agencies through the vetting process. The nature and scope of information that is made available by the Vetting Support Agencies is defined by pre-existing information sharing agreements between State, USCIS, and Vetting Support Agencies in concert with the Vetting Information Sharing and Technical-assistance Agreement (VISTA) agreed to by those agencies and approved by the National Vetting Governance Board.

Privacy Risk: There is a risk that USCIS Refugee Officers may make decisions to grant or deny an application for refugee resettlement based on inaccurate information identified during the NVC process.

Mitigation: This risk is partially mitigated. Information is collected directly from

[66] Refugee Case Records, STATE-59, 77 Fed. Reg. 5865 (Feb. 6, 2012).
[67] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 Fed. Reg. 43556 (Sep. 18, 2017).
[68] DHS/USCIS-008 Refugee Access Verification Unit, 78 Fed. Reg. 70313 (Nov. 25, 2013).
[69] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 Fed. Reg. 36950 (July 31, 2018).
[70] DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 Fed. Reg. 72075 (Oct. 19, 2016).
[71] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 Fed. Reg. 47411 (Aug. 8, 2012).

applicants during the application process for refugee resettlement, ensuring a high level of accuracy upon collection. However, if an applicant for refugee resettlement provides inaccurate information, it may result in inaccurate results from the NVC process. Referral partners (including UNHCR, U.S. Embassies, or the applicant themselves in some cases) provide initial data, and Bureau of Population, Refugees, and Migration -funded Resettlement Support Center workers confirm data in pre-screening applicants. USCIS Refugee Officers interview all applicants during the application process and can ask questions to resolve potential identity matching issues and other discrepancies. Further, Vetting Support Agencies are required to apply their analytic standards to ensure that information regarding the applicant is objective, timely, relevant, and accurate. For example, Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive 203, which requires that personally identifiable information is disseminated "only as it relates to a specific analytic purpose . . . [and] consistent with IC element mission and in compliance with IC element regulation and policy, including procedures to prevent, identify, and correct errors in PII."[72] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any factors affecting source quality and credibility.[73]

The recommendations provided by USCIS Vetting Analysts may inform, but do not determine the outcome of an application's adjudication. It is the responsibility of USCIS's Refugee Officers to evaluate the substance and assessed reliability of the information provided by Vetting Support Agencies in conjunction with other information available to them when determining whether to approve or deny an application for refugee resettlement.

Privacy Risk: There is a risk that USCIS Refugee Officers will make adjudications based solely on Vetting Analysts' recommendations and not on all the appropriate information available to them.

Mitigation: This risk is mitigated. The goal of the NVC process is not to make an adjudication on behalf of USCIS, but rather to provide a recommendation based on a consolidated view and analysis of the vetting responses and information made available by the Vetting Support Agencies. USCIS Refugee Officers will base their adjudications on the totality of the information available to them, including information in the application and supporting documentation, other contents of the applicant's A-File, the results of USCIS's security checks, general information about country conditions that is relevant to the applicant's claim, and the USCIS Refugee Officer's interview of the applicant and derivative applicants.

The USCIS Refugee Officer may base a denial on information identified through or outside of the NVC process and technology and for reasons unrelated to national security, such as fraud or inadmissibility. At all times, the USCIS Refugee Officer makes the final determination to approve or deny refugee status based on the application of statutory criteria.

Uses of the Information

[72] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.
[73] *See* https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

USCIS will continue to use the information included in an individual's application for refugee resettlement to determine the eligibility of the foreign national to travel to the United States, including whether the applicant(s) may pose a risk to public safety or national security under the provisions of the INA. With the addition of the vetting support provided through the NVC process, USCIS will be better equipped to identify ineligible applicants, thereby enhancing national security while also better facilitating refugee resettlement.

USCIS will continue to employ unclassified vetting processes, document reviews, and applicant interviews to inform its adjudications in addition to the vetting against classified holdings that takes place through the NVC process. Information provided to USCIS through the NVC process will help to streamline USRAP application, vetting, and adjudication processes.

The sharing and use of information made available to USCIS by the Vetting Support Agencies is governed by the information sharing agreements in place between those agencies, the classified NVC/Intelligence Community Support Element Concept of Operations, and Vetting Support Agency-specific guidelines and policies applicable to the sharing of intelligence, law enforcement, or other information. USRAP Vetting Support Agencies that are elements of the Intelligence Community must determine that sharing intelligence with USCIS is permitted under their Attorney General-approved Intelligence Oversight Guidelines for the protection of U.S. person information, which are mandated by Executive Order 12333, and applicable internal policies and procedures before they may provide it to USCIS through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of USRAP data during the application process are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of USRAP application data, as documented in System of Records Notices, Privacy Impact Assessments, Privacy Act Statements or Privacy Notices, and applicable information sharing agreements, are reviewed as a part of the NVC process to on-board a new vetting program to ensure they are accurate and adequately support the vetting activities. This will help to ensure that individuals who provide the information receive adequate public notice of the purposes for which the data is collected and how it is used.

Notice

Notice is provided primarily via publicly available System of Records Notices and Privacy Impact Assessments published by both DHS and State. Refugee applicants and their family members who are listed on a refugee resettlement application are required to acknowledge or sign a notice of confidentiality, which notifies refugee applicants of all different parties with whom refugee application data is shared, including U.S. government partners for the purposes of security vetting. At all times, vetting records created through the NVC process and technology are covered by the provisions of the Immigration Biometric and Background Check System of Records Notice (DHS/USCIS-018) and the Refugee Case Processing and Security Screening System of Records Notice (DHS/USCIS-017). The refugee application, supplemental evidence, and supporting

documentation are maintained in State's refugee case management system, which is governed by State's Refugee Case Records System of Records Notice (STATE-59); in the applicant's USCIS A-File, which is governed by the A-File System of Records Notice (DHS/USCIS/ICE/CBP-001); and in USCIS systems governed by the Refugee Access Verification Unit SORN (DHS/USCIS-008). The Immigration Biometric and Background Check System of Records Notice (DHS/USCIS-018) and the Refugee Case Processing and Security Screening System of Records Notice (DHS/USCIS-017) govern the information collected, used, and maintained as part of the adjudication process, including decisional information. Finally, USCIS's Fraud Detection and National Security Directorate may review certain applications of individuals for potential fraud, public safety, and national security concerns. The Fraud Detection and National Security System of Records Notice (DHS/USCIS-006) governs how Fraud Detection and National Security creates and uses information during those reviews.

The Refugee Case Processing and Security Vetting Privacy Impact Assessment (DHS/USCIS/PIA-068) examines the collection, use, and maintenance of information by USCIS in support of refugee resettlement and employment eligibility. State's Refugee Processing Center START and Amazon Web Services Government Cloud (AWS GovCloud) and START Privacy Impact Assessments examine State's primary case management systems for tracking and processing applications for refugee resettlement.

Privacy Risk: There is a risk that applicants and other individuals whose PII is included in an application for refugee resettlement may not be aware and did not consent to their PII being used for vetting purposes.

Mitigation: This risk is partially mitigated. The USRAP application process asks the applicant(s) for information about individuals who may be unaware of the application or uninvolved in its completion. There is no means by which State or USCIS may provide notice to these individuals because they are unlikely to directly participate in completing the USRAP application. However, this Privacy Impact Assessment and the System of Records Notices cited above serve as notice to the public regarding the USRAP and that the NVC facilitates the vetting of refugee application data. Additionally, each application for refugee resettlement contains a Privacy Notice detailing USCIS's authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS.

Data Retention by the Project

USCIS owns and maintains the official record copy of the refugee vetting record stored in the NVC technology and retained in accordance with the applicable USCIS records schedule, which mandates a retention period of 100 years from the individual's date of birth.[74] The NVC technology maintains copies of the refugee vetting record data for five years from the date that the NVC receives

[74] NARA Disposition Authority Number DAA-0563-2013-0001-0005. To calculate the retention period for vetting records within the NVC technology, USCIS will use the date of birth of the subject of the vetting request if one is available. Typically, USCIS will have dates of birth for the primary applicant and any derivative applicants. For records in the NVC technology where there is no date of birth for the subject of the vetting request, USCIS will use the primary applicant's date of birth to calculate the retention period.

the vetting request. At all times, the refugee vetting records held in the NVC technology are maintained, used, and shared in accordance with the provisions of the relevant System of Records Notices.

Individual Vetting Support Agencies may also maintain internal records reflecting the results of the automated and manual reviews sent forward to the NVC. Where a Vetting Support Agency has identified and confirmed an analytically significant match related to a vetting request, the Vetting Support Agency may retain that information as authorized by applicable Attorney General-approved Guidelines or as law enforcement information pursuant to the Vetting Support Agency's record control schedules. In no event shall a Vetting Support Agency retain vetting request information not determined to constitute an analytically significant match for longer than three years (USCIS's retention period for this data).

Privacy Risk: There is a risk that Vetting Support Agencies will retain information from Vetting Support Requests for longer than is necessary.

Mitigation: This risk is mitigated. Existing and new information sharing agreements between Adjudicating Agencies and Vetting Support Agencies that define the retention of data are reviewed by the NVC's Legal Working Group and Privacy, Civil Rights, and Civil Liberties (PCRCL) Working Group prior to the on-boarding of any new vetting programs to the NVC process. These information sharing agreements are reviewed along with the retention periods outlined in applicable Privacy Impact Assessments, System of Records Notices, record retention schedules, and Attorney General-approved Guidelines. These reviews aim to ensure that retention policies are appropriate and balance the U.S. Government's need to retain the data for operational purposes and afford effective redress against the risks to individuals that lengthy retention periods may create (e.g., data breaches and the possible adverse consequences of relying on aging, inaccurate data).

Additionally, the retention period for the vetting support records applicable to each vetting program is documented internally in classified documents that outline the specific processes for those particular vetting programs. This documentation defines the authorized retention period of Vetting Support Requests shared with Vetting Support Agencies and the purposes for such sharing. Vetting Support Agencies may retain vetting records for longer periods when, for example, they are identified as foreign intelligence or are relevant to law enforcement investigations in accordance with existing information sharing agreements, applicable law, and policy.

For Vetting Support Request information ingested by Vetting Support Agencies' internal systems, this risk is not fully mitigated solely by NVC technologies. This risk is further mitigated by the internal retention controls of the Vetting Support Agencies, including records retention schedules, the National Security Act of 1947, and Executive Order 12333-derived retention limitations.

Information Sharing

Neither National Security Presidential Memorandum (NSPM)-9[75] nor the NVC provide any new legal authority to State, DHS, or Vetting Support Agencies to collect, retain, store, or use information regarding applications for refugee resettlement. All refugee vetting activities using the NVC process and technology are based on existing legal authorities. State and DHS will continue to share information with other federal counterterrorism partners. Existing information sharing and access agreements supporting these vetting arrangements have been reviewed by State, DHS, and the appropriate Vetting Support Agencies to ensure all legal, privacy, civil rights, and civil liberties requirements are satisfied regarding the sharing and use of information in the NVC process. The classified Addendum to the NVC/Intelligence Community Support Element Concept of Operations also contains provisions that govern the scope of information sharing and prescribe appropriate information sharing safeguards.

State has determined that disclosure of data to Vetting Support Agencies to provide vetting support services is compatible with the purposes for which the data was collected. These information sharing agreements and the classified NVC/Intelligence Community Support Element Concept of operations have established the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and appropriate privacy protections for the data.

Privacy Risk: There is a risk that the NVC process will result in information being shared with Vetting Support Agencies that do not have authority to support vetting activities or do not have data relevant to adjudications of applications for refugee resettlement based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the PCRCL Working Group supporting the National Vetting Governance Board are charged with ensuring NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the NVC Implementation Plan and reviewed the NVC's technical designs, plans, and deployment to ensure they meet all legal and PCRCL requirements. These reviews included an evaluation by the working group members, which include representatives from Vetting Support Agencies, State, and DHS to ensure that the vetting does not exceed the legal authorities of State, DHS, or the Vetting Support Agencies. In addition, agency legal counsel and PCRCL offices at State, DHS, and the Vetting Support Agencies are engaged in reviews of the same issues to ensure their agencies are complying with applicable laws and PCRCL policies, standards, and practices.

Redress

The NVC does not possess the authority to collect, retain, use, or share information of its own and therefore does not provide any specific redress process. The NVC defers to the process or processes that Adjudicating Agencies and data owners employ to provide redress to individuals

[75] *See* https://www.whitehouse.gov/presidential-actionas/presidential-memorandum-optimizing-use-federal-government-information-support-national-vetting-enterprise/.

regarding their decisions and adjudications, where applicable.

When USCIS denies a refugee application, it provides the applicant a "Notice of Ineligibility for Resettlement" that generally will indicate the legal basis for the denial. There is no appeal for a denial of an application for refugee resettlement. USCIS may, however, exercise its discretion to review a case if an applicant files a "Request for Review" with the assistance of the Resettlement Support Centers that processed their application.

Privacy Risk: There is a risk that individuals will not have the ability to contest an adjudication that used information provided through the NVC process and technology as part of the determination

Mitigation: This risk is partially mitigated by the ability of an applicant to file a "Request for Review" of the denial of an application for refugee resettlement. USCIS may exercise its discretion to conduct a review of the case in question. The NVC defers to the process or processes that Adjudicating Agencies and data owners employ to provide redress to individuals regarding their decisions and adjudications, where applicable.

Auditing and Accountability

All personnel must undergo appropriate training before accessing the NVC technology, including classification and data protection training. Additionally, all personnel seeking access to refugee data in the NVC technology must undergo targeted confidentiality training related to the handling of special protected class data.

The NVC process and technology includes an audit function that captures electronic messages and transactions within its own technology and with other systems involved in the vetting workflow. It has the capability to fully review the actions that occurred in the workflow, beginning with the original Vetting Support Request, through all vetting responses, to any USCIS Vetting Analyst recommendations. The format and location of these records permits the reporting of metrics, support of redress processes (where applicable), and retrieval of records for compliance and oversight purposes.

United States Refugee Admissions Program (USRAP) Supplement

Refugee Vetting and Travel Initiative

Last updated September 2, 2022 (back to top)

The U.S. government continues to support vulnerable Afghans as they attempt to safely resettle in the United States through various programs, including the U.S. Refugee Admissions Program (USRAP). However, given the current safety and security circumstances in Afghanistan, the Department of State (DOS) is initiating vetting checks via established USRAP vetting mechanisms, including the National Vetting Center (NVC), for refugee applicants within Afghanistan and certain surrounding locations, which will allow the U.S. government to prioritize these applicants for U.S. government-facilitated relocation to a secondary location.

Applicants whose vetting check results do not produce any analytically significant threat information that may affect their eligibility for refugee status may be prioritized for relocation to a secondary location. Once the applicant arrives at the secondary location, they will continue through their USRAP processing, including their applicant interview, medical screenings, and other routine USRAP procedures. Applicants whose vetting checks results in matches to analytically significant threat information will not be prioritized for relocation to a secondary location. Instead, they will continue processing through the USRAP in their host country.

The NVC is publishing this USRAP Supplement on the *Refugee Vetting and Travel Initiative* for transparency purposes only. There are no new privacy risks to the NVC's USRAP PIA Addendum related to this initiative.

Responsible Officials

Monte Hawkins
Director
National Vetting Center
Department of Homeland Security

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
Department of Homeland Security

NVC PIA Addendum 4:

Advance Travel Authorization (ATA)

Last updated October 24, 2022 (back to top)

This Addendum outlines the process, referred to as Advance Travel Authorization (ATA), through which the National Vetting Center facilitates vetting by the U.S. Department of Homeland Security (DHS) of noncitizens from certain countries who are requesting authorization to travel to the United States to seek a discretionary grant of parole as part of discrete initiatives.[76] The ATA vetting process ensures that appropriate screening and vetting is conducted so that CBP adjudicators can make fully informed decisions regarding requests for travel authorization under the specific initiatives supported by ATA. Additional information about which initiatives receive vetting through this process is included in Appendix A.

Only individuals seeking travel authorization under one or more of the specific initiatives identified in Appendix A will be subject to screening and vetting using the ATA process and technology as described below.

ATA Process

The screening and vetting process for individuals in the ATA process is as follows. First, a supporting individual or entity legally present in the United States (U.S. supporter) will submit a signed declaration of financial support (Form I-134) via the *myUSCIS* portal.[77] This declaration will include the U.S. supporter's biographic information as well as that of the foreign national(s) and eligible family members whom they intend to support (beneficiary).[78] U.S. Citizenship and Immigration Services (USCIS) conducts the appropriate financial verification and background checks on the U.S. supporter. Following USCIS's confirmation of the U.S. supporter's eligibility, the beneficiary will receive an electronic message from USCIS inviting them to create a *myUSCIS* account.[79] Once in *myUSCIS*, the beneficiary or beneficiaries will be required to review their biographic information and attest to completion of all additional requirements.

Once the *myUSCIS* enrollment process is complete, a copy of the beneficiaries' biographic and biometric data[80] is sent to the Automated Targeting System (ATS) maintained by U.S. Customs

[76] See Appendix A for the list of initiatives for which DHS is employing ATA as a vetting process. The decision to parole a noncitizen into the United States is made at the port of entry, on a case-by-case basis, pursuant to the Immigration and Nationality Act (INA) section 212(d)(5), 8 U.S.C. 1182(d)(5).
[77] The *myUSCIS* portal may be found at https://my.uscis.gov.
[78] Eligible family members include immediate family members of the principal who are traveling with that beneficiary. For purposes of this process, immediate family members are limited to a spouse, common-law partner, and/or unmarried child(ren) under the age of 21. A separate Form I-134 is require for each traveler and eligible family member.
[79] *See* DHS/USCIS/PIA-071 MYUSCIS ACCOUNT EXPERIENCE and subsequent updates, *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[80] NVC classified vetting is completed using only biographic selectors collected about the beneficiary or beneficiaries on the I-134.

and Border Protection (CBP),[81] where it is vetted against select DHS and other federal agency security and law enforcement databases for national security, border security, public health, and public safety concerns. CBP conducts this vetting to determine whether the beneficiary poses a security risk to the United States and whether they are eligible to obtain advance authorization to travel to the United States to seek a discretionary grant of parole. This process will include classified vetting facilitated by the process and technology of the National Vetting Center (NVC).

NVC Support to ATA

All ATA-eligible travelers and other eligible beneficiaries between the ages of 14-79 whose information is submitted via USCIS's Form I-134 will be vetted through the NVC process and technology. The NVC process and technology described in the full NVC PIA above will be used to facilitate the vetting of ATA data, helping to ensure CBP is informed by all appropriate responsive information held by appropriate Vetting Support Agencies within the U.S. Government.

The starting point for vetting of all beneficiaries whose information is provided via Form I-134 is the transmission of a Vetting Support Request, consisting of beneficiaries' biographic data, to Vetting Support Agencies.[82] The documentation approved by the National Vetting Governance Board that will authorize this vetting support reflects the terms and conditions of information sharing and vetting support for this initiative as agreed to by all departments and agencies participating in the initiative and specifies which available data fields are included in the Vetting Support Request and how they are delivered to each Vetting Support Agency. CBP Vetting Analysts use NVC technology to receive and review any Vetting Support Response for which there is a relevant and appropriate classified or unclassified record made available by the Vetting Support Agencies. CBP Vetting Analysts develop a recommendation to either grant or deny the request for advance travel authorization based on their analysis of this information. CBP Adjudicators then review the recommendation, any relevant analyst notes provided by the CBP Vetting Analyst, and any additional unclassified information available to make their final decision to grant or deny the advance authorization for travel.

The NVC's process and technology will allow for the following:

- Distribution of Vetting Support Requests (*i.e.,* data from all Form I-134 submissions) to Vetting Support Agencies;
- Receipt and distribution of Vetting Support Responses from Vetting Support Agencies to CBP;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for CBP Vetting Analysts to access classified and unclassified records identified by a Vetting Support Agency as relevant to a Vetting Support Request;

[81] *See* DHS/CBP/PIA-006 AUTOMATED TARGETED SYSTEM and subsequent updates, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[82] As explained in the PIA, the NVC does not make recommendations or adjudications. Its role is limited to that of facilitator or service provider of the NVC process and technology used to facilitate vetting by CBP.

- Support for CBP Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Managing access to data by individual users and infrastructure according to pre-determined rules and standards;
- Managing the retention of data according to approved record schedules and information sharing agreements;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for established redress processes, FOIA requests, discovery in litigation, and other data retrieval requirements.

Privacy Impact Analysis

Authorities and Other Requirements

USCIS collects Form I-134 information pursuant to the Immigration and Nationality Act (INA), section 101, and 8 U.S.C. § 1182(d)(5). Pursuant to 8 U.S.C § 1182(d)(5), the Secretary of Homeland Security has the authority and discretion to parole noncitizens into the United States temporarily for urgent humanitarian reasons or significant public benefit.[83] Pursuant to 8 C.F.R. § 212.5(f), DHS may issue an "appropriate document authorizing travel" to a noncitizen without a visa who is travelling to the United States to seek parole. System of Records Notice (SORN) coverage for information collected via Form I-134 is provided by DHS/USCIS-001 – Alien File, Index, and National File Tracking System and by DHS/USCIS-007 – Benefits Information System.[84]

CBP ATS derives its authority primarily from 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 8 U.S.C. § 1357; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107-173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). See also, e.g., 6 U.S.C. §§ 111, 211; 8 U.S.C. §§ 1103, 1182, 1225, 1225a, 1324; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623, 1624, 1644, 1644a. SORN coverage for ATS is provided by DHS/CBP-006 Automated Targeting System.

The use of the NVC process and technology for the ATA vetting process does not provide any new legal authorities for CBP to collect, retain, store, or use information, or to make adjudications based on vetting. All screening and vetting activities facilitated through the NVC process are based on CBP's existing legal authorities. ATA Vetting Support Agencies similarly are

[83] The Immigration and Nationality Act (INA) allows authorized DHS officials to use their discretion to parole any noncitizen applicant for admission into the United States temporarily for urgent humanitarian reasons or significant public benefit. (See 8 U.S.C. § 1182(d)(5); 8 C.F.R. § 212.5). An individual who is paroled into the United States has not been admitted into the United States for purposes of immigration law.

[84] See generally DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (October 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns; DHS/USCIS-007 Benefits Information System, 84 FR 54622 (October 10, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.

engaged in the vetting process pursuant to their existing legal authorities.

Characterization of the Information

The USCIS Form I-134 collects biographic information about beneficiaries that will be used to develop Vetting Support Requests that will be sent to the Vetting Support Agencies. To make a final adjudication on a beneficiary's advance authorization to travel, CBP will receive a recommendation generated by CBP Vetting Analysts who, acting under CBP authorities, analyze information made available by Vetting Support Agencies. The nature and scope of information that is made available by the Vetting Support Agencies is defined by the documentation approved by the National Vetting Governance Board that authorizes this vetting support, which is attached as an addendum to the classified NVC Concept of Operations (CONOP).

Privacy Risk: There is a risk that CBP may make decisions to grant or deny an advance authorization to travel based on information identified during the NVC process that is inaccurate.

Mitigation: This risk is partially mitigated. Information collected about the beneficiary via Form I-134 is provided by the U.S. supporter and not by the beneficiary themselves. This risk is partially mitigated because the beneficiary will have the opportunity to review the accuracy of their information via the *myUSCIS* portal prior to being transmitted to the NVC. However, if an individual seeking advance authorization to travel provides inaccurate information, it may result in inaccurate results from the NVC process.

When beneficiary information is provided, Vetting Support Agencies are required to apply their analytic standards to ensure that any information disseminated to CBP regarding the beneficiary is objective, timely, relevant, and accurate. For example, Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive 203, which requires that PII is disseminated "only as it relates to a specific analytic purpose . . . [and is] consistent with IC element mission and in compliance with IC element regulation and policy, including procedures to prevent, identify, and correct errors in PII."[85] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any factors affecting source quality and credibility.[86]

The recommendations provided by the CBP Vetting Analysts inform, but do not determine, the outcome of the request for advance authorization to travel. It is CBP's responsibility to evaluate the substance and assess the reliability of the additional information provided by the Vetting Support Agencies, in conjunction with other information available to the CBP Adjudicator in determining whether to approve or deny an application.

Privacy Risk: There is a risk that CBP will make decisions based solely on the Analyst's Recommendation and not all appropriate information available to the CBP Adjudicator.

Mitigation: This risk is mitigated. The goal of the NVC process is not to make an adjudication for CBP, but rather to provide a recommendation based on a consolidated view and

[85] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.
[86] *See* https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

analysis of the Vetting Support Responses and information made available by the Vetting Support Agencies. CBP Adjudicators will still conduct other appropriate vetting activities outside of the NVC process using ATS and other systems, ensuring that the final adjudication will be holistically based on all information about the noncitizen that is available.

CBP will also have access to NVC technology to view the Vetting Record, including the Vetting Support Responses, underlying information, and Analyst Notes, before making the final decision on the advance travel authorization.

Uses of the Information

CBP will use the information to determine the eligibility of the beneficiary to travel to the United States, including whether the individual poses a threat to national security, border security, public health, or public safety. With the addition of the vetting support provided through the NVC process, CBP will be better equipped to identify travelers of interest and distinguish them from those who do not pose a higher risk, thereby improving its screening and vetting capabilities while also more efficiently facilitating the travel of those who do not pose a risk.

CBP will continue to vet beneficiary information against selected security and law enforcement databases at DHS outside of the NVC process, while also employing the NVC process and technology to compare against Vetting Support Agencies' holdings as well.The sharing and use of information made available to CBP by Vetting Support Agencies is governed by the documentation approved by the National Vetting Governance Board that authorizes this vetting support, which is attached as an addendum to the classified NVC CONOP, along with the Vetting Support Agencies' guidelines and policies applicable to the sharing of intelligence, law enforcement, or other information. Vetting Support Agencies that are elements of the Intelligence Community must determine that sharing intelligence with CBP is permitted under their Attorney General Guidelines for the protection of U.S. person information, which are mandated by Executive Order 12333 and other applicable procedures, before they may provide it to CBP through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of data via Form I-134 are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of the data are defined in publicly available documents such as the Privacy Notice (provided to individuals submitting information via Form I-134), USCIS's Benefits Information System and Alien File, Index, and National File Tracking System of Records SORNs, CBP's ATS SORN, the ATS PIA, CBP's ATA PIA,[87] and the National Vetting Center PIA (to include this Addendum). These documents clearly state that the information collected via Form I-134 will be used for screening and vetting purposes.

All vetting activities conducted via the NVC process and technology are clearly defined and

[87] *See* DHS/CBP/PIA-073 ADVANCE TRAVEL AUTHORIZATION, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

governed by documentation approved by the National Vetting Governance Board that authorizes this vetting support, which is attached as an addendum to the classified NVC CONOP.

Notice

U.S. supporters who provide information through Form I-134 do so voluntarily and after having the opportunity to review the Privacy Notice, so it is expected they are fully aware that they are submitting the information to DHS, that the submission of the information is voluntary, how DHS intends to use that data, the authorities under which it is collected, and that not providing the information may affect the Department's final decision or result in denial of their affidavit.

Privacy Risk: There is a risk that beneficiaries may not be aware and did not consent to their PII being used for vetting purposes.

Mitigation: This risk is partially mitigated because Form I-134 collects information about beneficiaries who may not be aware of the process or participate in its completion. However, the beneficiary is notified by USCIS of the U.S. sponsor's Form I-134 submission. The beneficiary must also create a *myUSCIS* account in order to continue to the screening and vetting stage of the ATA process. In addition, DHS has taken a number of steps to provide general public notice of the ATA process, including by publishing notice in the Federal Register of initiatives supported by the ATA vetting processing that references national security and public safety vetting, this PIA Addendum, CBP's ATA PIA, and additional U.S. Government messaging.

If an individual who did not provide their own information believes that DHS may have information about them that was submitted through Form I-134, that individual may seek to review this information by following the record access procedures described in USCIS's Alien File, Index, and National File Tracking System and Benefits Information System SORNs.

Data Retention by the Project

The NVC will retain vetting records, which include the Vetting Support Request, Vetting Support Response, Analyst Notes (if applicable), Analyst Recommendation, and Adjudication for a period of up to two years, which parallels the general parole period for individuals participating in the discrete initiatives outlined in Appendix A who are paroled pursuant to those discrete initiatives.

NCTC will provide recurrent vetting support during the initial 90 days following the issuance of authorization to travel to the United States to request parole under the ATA process. Additionally, NCTC will provide recurrent vetting support for the duration of parole (i.e., two years) on individuals who travel to the United States within 90 days of their authorization to travel. Vetting Support Agencies are separately authorized to maintain ATA Vetting Records outside the NVC process and technology if identified as retainable in accordance with its Attorney General Guidelines or identified by a law enforcement agency or administrative agency as retainable in a Privacy Act compliant system. In such cases, a record may be retained for a longer period in accordance with the applicable records retention schedules and individual authorities to retain the information.

Privacy Risk: There is a risk that vetting records will be retained longer than necessary as a result of the NVC process and technology.

Mitigation: This risk is mitigated. Unless an individual record is identified as permanently retainable by a Vetting Support Agency receiving the record in accordance with the documentation approved by the National Vetting Governance Board to, the retention period for the vetting record will not exceed two years. If the record is found to be retainable, it may be retained for a longer period by that Vetting Support Agency, but only in accordance with that agency's legal authorities and other applicable policies and procedures, including, for those Vetting Support Agencies that are elements of the Intelligence Community, the standards for collecting and retaining foreign intelligence information described in the agency's Attorney General Guidelines for the protection of U.S. person information, which are required by Executive Order 12333.

Privacy Risk: There is a risk that some individuals may gain U.S. Person (USPER)[88] status during this period and are not removed from recurrent vetting in a timely manner.

Mitigation: The risk is partially mitigated. Upon discovery of status change during an analyst's manual review at any time during recurrent vetting, the identified record is handled in accordance with the VSA's Attorney General Guidelines. Additionally, the NVC Privacy, Civil Rights, and Civil Liberties Officer will review initiatives underway within DHS with the goal of better assessing an individual's status and disseminating information when an individual changes status, such as when an individual becomes a U.S. person. Such sharing of information is important for removing individuals who have changed status from recurrent vetting. Within six months of publication of this PIA, the NVC Privacy, Civil Rights, and Civil Liberties Officer will present options for addressing beneficiary status change and their expected timelines for delivery to the NVC Privacy, Civil Rights, and Civil Liberties Working Group. The Working Group will then assess any potential concerns and work to mitigate them.

Information Sharing

Neither National Security Presidential Memorandum (NSPM)-9 nor the NVC provide any new legal authority to CBP, USCIS, or Vetting Support Agencies to collect, retain, store, or use information collected via Form I-134. All vetting activities using the NVC process and technology are based on existing legal authorities. The documentation supporting these vetting arrangements has been reviewed by CBP and the Vetting Support Agencies to ensure all legal, privacy, civil rights, and civil liberties requirements regarding the sharing and use of ATA beneficiary information in the NVC process are satisfied. This documentation and the classified Addendum to the NVC-Intelligence Community Support Element (ICSE) Concept of Operations have established the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy, civil rights, and civil liberties protections for the data.

[88] U.S. Persons (USPER) is defined as United States citizens, Lawful Permanent Residents, unincorporated associations substantially composed of United States citizens or permanent resident non-citizens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. S*ee* E.O. 12333, *United States Intelligence Activities*, 2008 as amended.

USCIS and CBP have determined that disclosure of beneficiary data to the Vetting Support Agencies to provide vetting support services is compatible with the purposes for which the data was collected and is authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3) (specifically, the routine uses set forth in the DHS/CBP-006 Automated Targeting System (especially Routine Uses G and H)).

Privacy Risk: There is a risk that the NVC process will result in information being shared with Vetting Support Agencies that do not have authority to support vetting activities or do not have data relevant to adjudications based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the PCRCL Working Group supporting the National Vetting Governance Board are charged with ensuring that NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the NVC Implementation Plan and reviewed the NVC's technical designs, plans, and deployment to ensure they meet all legal and PCRCL requirements. These reviews included an evaluation by the working group members, which include representatives from various Vetting Support Agencies and DHS, to ensure that the vetting does not exceed the legal authorities of either CBP or the Vetting Support Agencies. In addition, agency legal counsel and PCRCL offices at CBP, DHS, and the Vetting Support Agencies are engaged in continual reviews of the same issues to ensure their agencies are complying with applicable laws and PCRCL policies, standards, and practices.

Information sharing agreements are also in place to facilitate information sharing between CBP and the Vetting Support Agencies. These agreements have also been reviewed by appropriate oversight offices to ensure all legal and PCRCL requirements are being fulfilled.

Redress

The NVC does not possess the authority to collect, retain, use, or share information of its own and therefore does not provide any specific redress process. The NVC defers to the process or processes that Adjudicating Agencies employ to provide redress to individuals regarding their adjudications, where applicable

In the event of a redress inquiry, CBP will follow all applicable redress procedures established by DHS's Traveler Redress Inquiry Program (DHS TRIP)[89] and the CBP Redress Office. They will facilitate the review and assessment of any information identified during the NVC process, including by coordinating with relevant Vetting Support Agency partners, as appropriate, to ensure that the information used in the initial adjudication is still valid and determine if any updated information is available.

CBP and the Vetting Support Agencies will respond to requests for records in accordance with their applicable policies, practices, and procedures, including, but not limited to, responses to requests submitted by Congress, the Government Accountability Office, or members of the public under the Privacy Act, FOIA, or Judicial Redress Act. Any such requests to CBP for Vetting Support

[89] For more information about DHS TRIP, please *see* https://www.dhs.gov/dhs-trip.

Agency responses provided in response to Vetting Support Requests will be coordinated with those agencies prior to response, and any request for data provided to a Vetting Support Agency as a Vetting Support Request will be coordinated by that agency with CBP prior to response. To the extent permissible under applicable law, the agency receiving the request will defer to the data originator for a determination as to the proper response. If non-attribution for a response provided by a Vetting Support Agency is, in that agency's conclusion, appropriate, CBP will respond to the request without attribution to the Vetting Support Agency, thereby protecting the source of the information from disclosure.

Privacy Risk: There is a risk that individuals will not have the ability to contest a decision that used information provided through the NVC process and technology as part of the determination.

Mitigation: This risk is partially mitigated. This PIA Addendum as well as the ATS PIA provide options for redress including the DHS TRIP process described above. The NVC defers to the process or processes that Adjudicating Agencies and data owners employ to provide redress to individuals regarding their decisions, where applicable

Auditing and Accountability

The NVC process and technology includes an audit function that captures electronic messages and transactions within its own technology and with other systems involved in the vetting workflow. It has the capability to fully review the actions that occurred in the workflow, beginning with the original Vetting Support Request, through all Vetting Support Responses, to any Analyst Recommendations. The format and location of these records permits the reporting of metrics, support of redress processes, and retrieval records for compliance and oversight purposes.

Responsible Officials

Monte Hawkins
Director
National Vetting Center
Department of Homeland Security

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
Department of Homeland Security

APPENDIX A:

Initiatives receiving screening and vetting support through the ATA or similar processes:

1. *Uniting for Ukraine* (U4U) Parole Process.
2. Venezuelan Parole Process announced on October 12, 2022.
3. Nicaragua Parole Process announced on January 5, 2023.
4. Cuba Parole Process announced on January 5, 2023.
5. Haiti Parole Process announced on January 5, 2023.
6. Family Reunification Process (FRP) announced on July 7, 2023. The Secretary of Homeland Security announced several new and expanded parole processes intended to create a more streamlined, safe, and orderly process for individuals of certain nationalities, who already possess family-based immigrant petitions to request advance authorization to travel to the United States to seek a discretionary grant of parole. This includes the implementation of an FRP for Columbians, El Salvadorians, Guatemalans, and Hondurans as well as updates to modernize the Cuba Family Reunification Parole (CFRP) and the Haitian Family Reunification Parole (HFRP) processes. Additionally, the Family Reunification Parole Process for Ecuadorians was published in the Federal Register on November 16, 2023.
7. Ad Hoc ATA – In rare instances, an unforeseen, extreme, and rapid political, economic, or humanitarian event may lead the United States government to facilitate the travel of limited numbers of noncitizens to the United States on short notice. An Ad Hoc ATA initiative may be utilized to create a more streamlined, but limited duration, process to provide NVC vetting support prior to United States government authorization for individuals to travel to the United States to seek parole.

   This Ad Hoc ATA process permits certain U.S. government-sponsored noncitizens who lack visas or other appropriate entry documents, and their qualifying family members, to request advance authorization to travel to the United States to seek parole, provided they are deemed eligible by the sponsoring U.S. government agency. The key deviation from the ATA process described above relates to the initiation mechanism. Instead of a U.S. sponsor submitting an I-134 form via the *myUSCIS* portal as described above, the ATA Ad Hoc process is initiated by a U.S. government agency by providing the NVC with required information for individuals that are being sponsored to travel.

   The U.S. Government agency requesting Ad Hoc ATA vetting support is responsible for confirming eligibility for the initiative and must provide the NVC with traveler information no less than five (5) days prior to the planned travel. Vetting Support Agencies will provide reviewed responses within three (3) business days. Approved travel is valid for 90 days unless the beneficiary is subsequently determined to be ineligible to travel. The period for parole is two (2) years.

   The ATA Ad Hoc process has associated duration and volume limitations which limit its use to 1,000 vetting requests per day for a period of no more than ten days. Where an

initiative falls within those parameters, the NVC Director is required to notify the National Vetting Governance Board 24-hours in advance. Any initiative that exceeds those parameters requires additional review, approval, and documentation by the NVC Director and the National Vetting Governance Board, in conjunction with review by the National Vetting Governance Board's Legal, Privacy, Civil Rights, and Civil Liberties (PCRCL), and Technical Working Groups, before the ATA Ad Hoc process can be used to provide vetting support to the initiative.

NVC PIA Addendum 5:

U.S. Department of State's (State) Non-Immigrant Visa (NIV)

Last updated May 12, 2022 (back to top)

Under the Immigration and Nationality Act (INA), as amended and codified at Title 8 of the U.S. Code, an individual may not ordinarily travel to or enter the United States without appropriate documentation, such as a visa. Before issuing a visa, a Department of State (DOS or "State") Consular Officer must determine that an applicant qualifies for the classification of the visa sought and is not inadmissible under any provision of the INA. The INA sets forth numerous categories of inadmissibility for a visa, including a series of categories pertaining to criminal and related grounds and a separate series pertaining to security and related grounds, which includes grounds pertaining to terrorist activities. In all instances, the ultimate determination to grant or deny a visa resides with the Consular Officer stationed at a DOS post—usually, a U.S. Embassy or Consulate overseas.

Non-immigrant visas (NIV) are issued to foreign nationals seeking to enter the United States on a temporary basis for tourism, business, medical treatment, or certain types of temporary work. To evaluate whether an applicant qualifies for an NIV and is not inadmissible under any provision of the INA, State's Bureau of Consular Affairs (State/CA) is authorized to maintain direct and continuous relationships with security partners within the U.S. Government. For decades, State has leveraged this authority to support the review of NIV cases, in part through its Security Advisory Opinion (SAO) process. In the counterterrorism context, the SAO is an opinion generated by State/CA to inform Consular Officers' adjudication of a visa case where there is reason to believe—whether based on the Consular Officer's interactions with the applicant; the results of automated security checks against counterterrorism or other law enforcement, border security, or homeland security data; or due to broader circumstances surrounding the case—that additional information on the applicant would be useful in determining whether the applicant falls within one or more of the security-related categories of inadmissibility in the INA or other relevant provisions of U.S. law or policy.

National Vetting Center (NVC) Support to NIV Vetting

The NVC leverages the process and technology described in the NVC Privacy Impact Assessment above to facilitate the vetting of NIV application data, helping to ensure that State adjudications are informed by all appropriate responsive information held by NIV Vetting Support

Agencies in a timely and comprehensive manner. The starting point for the vetting of all NIV applicants through the NVC process and technology is the transmission of an NIV Vetting Support Request, which consists of NIV application data, to the NIV Vetting Support Agencies.[90] Existing memoranda of agreement (MOA) between State and the various Vetting Support Agencies determine which data fields in the application are included in the Vetting Support Request and how they are delivered to each Vetting Support Agency.

The NVC facilitates the process through which NIV Vetting Support Agencies make available Vetting Support Responses for review by State. State Vetting Analysts use NVC technology to receive and review any NIV Vetting Support Request for which there is a relevant and appropriate classified or unclassified record made available by the NIV Vetting Support Agencies. State Vetting Analysts develop a recommendation to either grant or deny the visa based on their analysis of this information. State Consular Officers at post then review the recommendation and any notes provided by the State Vetting Analyst, along with any additional unclassified information available, to make their final decision to grant or deny the NIV application.

The NVC's process and technology will allow for the:

- Distribution of Vetting Support Requests (i.e., data from all NIV applications) to NIV Vetting Support Agencies;
- Receipt and distribution of Vetting Support Responses from NIV Vetting Support Agencies to State;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for State Vetting Analysts to access classified and unclassified records identified by Vetting Support Agencies as relevant to a Vetting Support Request;
- Support for State Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Management of access to data by individual users and infrastructure according to pre-determined rules and standards;
- Management of the retention of data according to approved NIV record schedules and information sharing agreements;
- Logging of user activity for audit, oversight, and accountability purposes; and
- Support for NIV redress procedures, Freedom of Information Act (FOIA), 5 U.S.C. § 552, requests, discovery in litigation, and other data retrieval requirements.

<u>Department of State Access to U.S. Custom and Border Protection's (CBP) Electronic System for Travel Authorization (ESTA) for NIV Vetting</u>

Upon implementation of State's NIV program at the NVC, State Vetting Analysts will

[90] As explained in this Privacy Impact Assessment, the NVC does not make recommendations or adjudications. Its role is limited to that of facilitator or service provider of the NVC process and technology used to facilitate vetting and adjudications by State.

also be able to view CBP's ESTA vetting records within the NVC technology to support the NIV program.[91] ESTA applicants that are denied authorization for travel to the United States under the Visa Waiver Program (VWP)[92] are instructed that they may apply for a visa. Accordingly, State expects that many visa applicants from VWP countries will have previously applied for an ESTA. As a result, State will utilize information contained in ESTA vetting records within the NVC technology to further their analysis of pending NIV applications, as appropriate.

State Vetting Analysts will be granted read-only access to denied ESTA vetting records within the NVC technology, through the following process:

- Following the NVC's receipt of a "red" message to indicate a match against at least one of the other Vetting Support Agency's intelligence or law enforcement holdings occurred at the automated comparison stage, the NVC will send an initial red message to CBP's Automated Targeting System (ATS).[93]
- Upon receipt of this message, the Automated Targeting System will search its existing holdings to identify if the NIV applicant has a previously denied ESTA application.
- If the Automated Targeting System identifies an NIV applicant as having previously been denied an ESTA, then the Automated Targeting System will send a message to the NVC that includes the NIV application number and the denied ESTA application number.
- If a Vetting Support Agency follows up with a "Reviewed Red" message, the NVC technology will display a notification with the NIV record indicating the applicant had an ESTA application denied and provide State Vetting Analysts with the ESTA record number.

Once implemented, State Vetting Analysts will have access to all denied ESTA vetting records, including CBP Vetting Analyst and Adjudicator notes, within the NVC technology. State Vetting Analysts will be provided with read-only access to closed (i.e., adjudicated) ESTA denials in the NVC technology to avoid intentional or inadvertent modification of the ESTA vetting record. Further, State Vetting Analysts will be unable to view or otherwise access vetting records for ESTA applications that are pending a final decision at CBP.

DHS/U.S. Immigration and Customs Enforcement (ICE) Support to NIV Vetting

The process described in this Privacy Impact Assessment and accompanying NIV Addendum to the NVC Concept of Operations (CONOPs) will replace the prior SAO process that

[91] *See* DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA) and subsequent updates, *available at* https://www.dhs.gov/privacy.
[92] *See* 8 C.F.R. § 217 (describing this program). The Visa Waiver Program (VWP), administered by DHS in consultation with the Department of State, permits citizens of certain countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those 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.
[93] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS) and subsequent updates, *available at* https://www.dhs.gov/privacy.

identifies certain NIV applications for additional scrutiny based on counter-terrorism concerns.[94] ICE's Office of Homeland Security Investigations has historically supported the SAO process and will serve as a Vetting Support Agency for the NIV program through the NVC moving forward. As a Vetting Support Agency, ICE will provide support to State by searching for analytically significant threat information (ASTI)[95] in DHS holdings relating to certain visa applications where there has already been an indication of terrorism or other threats to national security or public safety.

ICE does not review all NIV applications. Instead, it only reviews those applications that result in a match against intelligence or law enforcement holdings from Vetting Support Agencies that have authorized ICE to view their matches at the automated comparison stage. Once an automated match is received by the NVC, a message is sent to CBP's Automated Targeting System, which maintains a copy of the NIV application, to queue the NIV application in the Automated Targeting System's Unified Passenger (UPAX) interface.[96] Once the application is queued in Unified Passenger, an ICE analyst is then tasked with reviewing the application and conducting additional research within DHS holdings. Unified Passenger queries can access law enforcement, border crossing, and immigration data from various DHS systems, including, but not limited to CBP's TECS[97] and ICE's Enforcement Integrated Database.[98] The ICE analyst may also query ICE's Investigative Case Management System (ICM) for further information.[99] These queries are completed directly through the Investigative Case Management System, not through Unified Passenger. ICE analysts will not query any DHS classified information in conducting their research.

In addition to the reviews described above, ICE analysts will also review any "Discretionary SAOs" issued by State. Discretionary SAOs are created when a State Consular Officer determines that an additional level of scrutiny should be applied to an application based on case-specific factors, such as information uncovered during the applicant interview process. In such instances, ICE will provide the results back to the NVC technology for the State vetting analyst to review via the NVC interface.

Based on an ICE analyst's review, there are two potential outcomes: (1) If the ICE analyst confirms the presence of analytically significant threat information in DHS unclassified holdings, they will flag it in Unified Passenger. Unified Passenger will then send a "Reviewed Red" message

[94] *See* DHS/ICE/PIA-011(a) Visa Security Program Tracking System-Network, *available at* https://www.dhs.gov/privacy, which sets forth more information on ICE's role in the SAO process.
[95] Analytically significant threat information provides analytic insight into the threat posed by an individual or group, whether directly or indirectly, to national security, homeland security, border security, or public safety. Information contained in a Vetting Support Request that is linked to other information available to Vetting Support Agencies through the NVC process only qualifies as analytically significant threat information where the link is accurate and sufficiently analytically significant to warrant dissemination outside of the Vetting Support Agency consistent with the guidelines, processes, and procedures of the Vetting Support Agency identifying the information.
[96] Unified Passenger (UPAX) is a technology refresh that updates and replaces the older functionality of the legacy ATS-Passenger interface. Unified Passenger functionality improves the process and system that assists CBP Officers in identifying individuals who require additional inspection and making admissibility decisions regarding individuals seeking admission to the United States.
[97] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* https://www.dhs.gov/privacy.
[98] *See* DHS/ICE/PIA-015 Enforcement Integrated Database, *available at* https://www.dhs.gov/privacy.
[99] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), *available at* https://www.dhs.gov/privacy.

to the other agencies involved in the vetting process (including State), which will include a notes section in which the ICE analyst can provide additional information; (2) If the ICE analyst concludes that there is no analytically significant threat information in DHS unclassified holdings, then a "Reviewed Green" message will be sent.

State Vetting Analysts will review responses from all Vetting Support Agencies, including ICE, and begin the State Visa Office's process for making a recommendation on whether to refuse or issue the visa. That recommendation is ultimately sent from the Visa Office to the State Consular Officer, who has the authority to adjudicate the visa application.

Privacy Impact Analysis

Authorities and Other Requirements

State collects NIV application information pursuant to 5 U.S.C. § 301 (Secretary of State's authorities with respect to Management of the Department of State); 22 U.S.C. § 2651a (Organization of the Department of State); 22 U.S.C. § 3921 (Management of the Foreign Service); and 8 U.S.C. §§ 1101-1537 (INA). The creation of the NVC does not provide new legal authorities to State to collect, retain, store, or use information, or to make adjudications based on vetting. All activities undertaken through the NVC process are based on State's existing legal authorities. NIV Vetting Support Agencies similarly are engaged in the vetting process pursuant to their own existing legal authorities.

NIV case records are maintained in a number of DOS systems, but are subject to a single, comprehensive Privacy Act System of Records Notice (SORN) for all visa records: Visa records, State-39.[100] In addition to the applications, this System of Records Notice also covers their related forms; photographs; internal (within DHS) and external communications; internal correspondence and notes relating to visa adjudications; and information, including personally identifiable information (PII)[101] regarding applicants' family members, employers, and references (including U.S. citizens and lawful permanent residents (U.S. persons)).

Characterization of the Information

State will continue to collect the same information from NIV applicants through the application process. Importantly, this application information will continue to include a digital photograph of the applicant, which will be utilized in the same way it was prior to NIV's implementation at the NVC, except that these photographs will now be passed to NIV Vetting Support Agencies using the NVC's process and technology. NIV Vetting Support Agency analyst reviews are automatically triggered where a selector from an application appears to match to information already collected by vetting support partners, just as they were prior to the NVC. A significant part of the analytic review conducted by the analyst is determining whether the apparent

[100] Department of State System of Records Notice – Visa Records, STATE-39, 86 FR 61822, November 8, 2021.
[101] DHS defines "Personally Identifiable Information" or PII, as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

match concerns the same individual (i.e., whether the applicant is the same person flagged in the partner's holdings). At times, the biographic information available to the analyst is sufficient to confirm or disqualify the match, but there are also occasions where the biographic information is insufficient to make a determination either way (e.g., there may be more than one individual with the same name and date of birth). Where that occurs and the Vetting Support Agency's previously collected information includes a photograph of the individual whose biographic information matched to one or more biographic selectors in the NIV application, the analyst may compare the photograph included in the NIV application package against the photograph in the NIV Vetting Support Agency's collection to assist in determining whether the automated match was accurate. At no time does the NIV Vetting Support Agency engage in automated one-to-one or one-to-many matching of the biometrics, and the manual comparison of photographic information only occurs where there has already been an automated match of biographic selectors and the photographic comparison would supplement the analyst's review of the available biographic information.

Notably, State Consular Officers will continue to receive recommendations from State Vetting Analysts, albeit through a new process and technology. Specifically, State Vetting analysts will now view information related to NIV applicants and make recommendations to State Consular Officers through the NVC process and technology. These recommendations are generated by the State Vetting Analysts who, acting under State authorities, analyze information made available by NIV Vetting Support Agencies. The nature and scope of information that is made available by the NIV Vetting Support Agencies is defined by the NIV Concept of Operations agreed to by those agencies and approved by the National Vetting Governance Board.

Privacy Risk: There is a risk that State Consular Officers may make decisions to grant or deny a visa application based on inaccurate information identified during the NVC process.

Mitigation: This risk is partially mitigated. Information is collected directly from applicants during the NIV application process, ensuring a high level of accuracy upon collection. However, if an NIV applicant provides inaccurate information, it may result in inaccurate results from the NVC process. State Consular Officers have the opportunity during the visa application process to communicate with the applicant and ask questions to resolve potential identity matching issues. Furthermore, NIV Vetting Support Agencies are required to apply their analytic standards to ensure that information regarding the applicant is objective, timely, relevant, and accurate. For example, NIV Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive 203, which requires that personally identifiable information is disseminated "only as it relates to a specific analytic purpose . . . [and] consistent with [Intelligence Community (IC)] element mission and in compliance with IC element regulation and policy, including procedures to prevent, identify, and correct errors in [personally identifiable information]."[102] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any factors affecting source quality and credibility.[103]

[102] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.
[103] *See* https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

The recommendations provided by the State Vetting Analysts inform, but do not determine the outcome of a visa adjudication. It is the responsibility of State's Consular Officers to evaluate the substance and assessed reliability of the additional information provided by NIV Vetting Support Agencies in conjunction with other information available to them when determining whether to approve or deny an NIV application.

Privacy Risk: There is a risk that State Consular Officers will make NIV adjudications based solely on the State Vetting Analyst recommendation without considering all the appropriate information available to them.

Mitigation: This risk is mitigated. The goal of the NVC process is not to make an adjudication for State, but rather to facilitate a recommendation from State Vetting Analysts based on a consolidated view and analysis of the Vetting Support Responses and information made available by the NIV Vetting Support Agencies. State Consular Officers will base their adjudications on the totality of the information available to them, including classified and unclassified vetting processes, document reviews, and interviews.

State Vetting Analysts will make their recommendations based on whether the information provided by NIV Vetting Support Agencies meets the legal standard described in relevant sections of U.S. law—usually, the grounds of inadmissibility contained in section 212 of the INA, 8 U.S.C. § 1182. In cases in which the State Consular Officer believes that an analyst's recommendation of refusal is inconsistent with the totality of available information about the visa applicant, the officer can request a supplementary analysis of the analytically significant threat information in the context of all known facts. Ultimately, the decision to grant or deny a visa rests entirely in the discretion of the State Consular Officer.

Privacy Risk: There is a risk that State Vetting Analysts may have access to more ESTA vetting records, within the NVC technology, than is required to make a recommendation on an NIV application to a State Consular Officer.

Mitigation: This risk is mitigated. The NVC implements access control capabilities to ensure that State Vetting Analysts are limited to read-only access to denied ESTA vetting records within the NVC technology. Further, State Vetting Analysts will be unable to view or otherwise access vetting records for ESTA applications that are pending a final decision at CBP. Decisions about access to the data for the NIV program were incorporated into the NVC process and coordinated with the National Vetting Governance Board's Privacy, Civil Rights, and Civil Liberties (PCRCL) and Legal Working Groups.

Uses of the Information

State will continue to use the information included in an individual's visa application as well as their denied ESTA vetting records within the NVC technology, as appropriate, to determine the eligibility of the foreign national to travel to the United States, including whether the visitor poses a law enforcement or security risk. With the addition of the vetting support provided through the NVC process, State will be better equipped to identify travelers of interest and distinguish them from legitimate travelers, thereby improving its security capabilities while also facilitating the

travel of lawful visitors.

State will continue to employ unclassified vetting processes, document reviews, and applicant interviews in addition to the vetting facilitated through the NVC's process and technology. The addition of the State Vetting Analyst recommendation for State Consular Officers only enhances State's ability to mitigate security gaps present in previous NIV application, vetting, and adjudication processes.

The sharing and use of information made available to State by NIV Vetting Support Agencies is governed by the information sharing agreements in place between those agencies, the classified NVC/Intelligence Community Support Element Concept of Operations, and NIV Vetting Support Agency-specific guidelines and policies applicable to the sharing of intelligence, law enforcement, or other information. NIV Vetting Support Agencies that are elements of the IC must determine that sharing intelligence with State is permitted under their Attorney General Guidelines for the protection of U.S. person information, which are mandated by Executive Order 12333 and other applicable procedures, before they may provide it to State through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of NIV data during the application process are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of NIV application data, as documented in System of Records Notices, Privacy Impact Assessments, Privacy Act Statements or Privacy Notices, and information sharing agreements, are reviewed as a part of the NVC process to on-board a new vetting program to ensure they are accurate and adequately support the vetting activities. This helps to ensure that individuals who provide the information receive adequate public notice of the purposes for which the data is collected and how it is used.

Further, 8 U.S.C. § 1202(f) and interagency information sharing agreements limit the use of data beyond what is authorized and appropriate. Visa records and records containing information subject to § 1202(f) are marked with a prominent banner for notice purposes. Any uses of information protected under § 1202(f) that are not previously authorized under existing agreements require prior approval by State.

Notice

Individuals who complete an NIV application do so voluntarily and after having the opportunity to review the Privacy Notice. They are notified in writing that they are submitting the information to State, how that data will be used, and the authorities under which it is collected. However, the NIV application does require that the applicant provide information concerning a U.S. point of contact—specifically, a name, address, telephone number, and email address. The U.S. point of contact (as well as other individuals listed on the application) may be an individual, a company, or another entity like a hotel where the individual plans to stay. If it is an individual, it may be a U.S. person, who may not know that the NIV applicant provided their information during

the application process. Additionally, family members may not be aware that the applicant has provided their information on an NIV application.

Privacy Risk: There is a risk that applicants and other individuals whose personally identifiable information is included in an NIV application (e.g., U.S. points of contact) may not be aware and did not consent to their personally identifiable information being used for vetting purposes.

Mitigation: This risk partially mitigated. Because the NIV application process asks the applicant for information about individuals who may not be aware of the application or participate in its completion, this risk cannot be fully mitigated. There is no way for State to provide notice to these individuals because they are unlikely to be involved in the application itself and may not be aware of it. In lieu of this, a number of steps have been taken to provide general public notice of this fact, including the publication of this Privacy Impact Assessment Addendum by DHS and State's Overseas Consular Support Applications Privacy Impact Assessment,[104] the unclassified version of the NVC Implementation Plan,[105] and the Privacy Notice provided to the applicant at the time of application on the NIV form, DS-160.

If an individual who is not an NIV applicant believes that State may have information about them as part of the NIV application, they may seek to review this information by following the individual access, redress, and correction procedures described in both the State-39 System of Records Notice and the Redress portion of this document.

Data Retention by the Project

NIV vetting records stored within the NVC technology are duplicates of the official record copy, which is retained on State servers for the National Archives and Records Administration (NARA) approved retention periods. These copies of NIV vetting records are controlled by State and stored in NVC Services for 11 years from the date of visa record creation. At all times, the copies of NIV records held in State-controlled spaces in NVC Services are maintained, used, and shared according to the provisions of the State-39 System of Records Notice.

As reflected in the State-39 System of Records Notice, the retention period for NIV applications depends on the nature of the information and the disposition of the visa adjudication; however, all NIV application data is retained in State's Consular Consolidated Database for 25 years for issued NIVs and either 25 or 100 years for refused NIVs depending on the grounds for refusal. All State records pertaining to the issuance or refusal of visas, including NIV case records, are protected as confidential pursuant to 8 U.S.C. § 1202(f), but this statute permits the limited use of visa records for, among other purposes, the enforcement and administration of the INA, and other

[104] *See* Department of State's Overseas Consular Support Applications (OCSA) Privacy Impact Assessment, *available at* https://www.state.gov/wp-content/uploads/2019/05/Overseas-Consular-Support-Applications-OCSA-now-consist-of-.pdf.
[105] An unclassified version of the Plan to Implement the Presidential Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise (Aug. 5, 2018) is available at https://www.dhs.gov/sites/default/files/publications/NSPM-9%20Implementation%20Plan.pdf.

laws of the United States.[106]

Individual NIV Vetting Support Agencies may also maintain internal records reflecting the results of the automated and manual reviews sent forward to NVC Services. Retention periods for any such records are determined by the applicable records schedules for those agencies in accordance with existing information sharing agreements and its Attorney General Guidelines.

Privacy Risk: There is a risk that NIV Vetting Support Agencies will retain information from Vetting Support Requests for longer than is necessary.

Mitigation: This risk is mitigated. The Adjudicating Agencies and Vetting Support Agencies review applicable information sharing agreements that define the retention of data, in coordination with the NVC's Legal Working Group and Privacy, Civil Rights, and Civil Liberties Working Group, prior to the on-boarding of any new vetting programs to the NVC process. These information sharing agreements are reviewed along with retention periods outlined in applicable Privacy Impact Assessments, System of Records Notices, record retention schedules, and Attorney General Guidelines. These reviews aim to ensure retention policies are appropriate and balance the U.S. Government's need to retain the data for operational purposes and afford effective redress against the risks to individuals that lengthy retention periods may create (e.g., data breaches and the possible adverse consequences of relying on aging, inaccurate data).

Additionally, the retention period for the vetting support records applicable to each vetting program is documented internally in classified documents that outline the specific processes for those particular vetting programs. This documentation defines the authorized retention period of Vetting Support Requests shared with NIV Vetting Support Agencies and the purposes for such sharing. Vetting Support Agencies may retain vetting records for longer periods when, for example, they are identified as foreign intelligence or are relevant to law enforcement investigations in accordance with existing information sharing agreements, applicable law, and policy.

For Vetting Support Request information ingested by NIV Vetting Support Agencies' internal systems, this risk is not fully mitigated solely by NVC technologies. This risk is instead further mitigated by the internal retention controls of the Vetting Support Agencies, including records retention schedules, the National Security Act of 1947, and Executive Order 12333-derived retention limitations.

Information Sharing

Neither National Security Presidential Memorandum (NSPM)-9 nor the NVC provide new legal authority to State or NIV Vetting Support Agencies to collect, retain, store, or use NIV information. All vetting activities for NIV using the NVC process and technology are based on existing legal authorities. State will continue to share NIV information in bulk with other federal counterterrorism partners. Existing external information sharing and access agreements supporting these vetting arrangements have been reviewed by State and the NIV Vetting Support Agencies to

[106] As used in this context, the designation "confidential" does not relate to the security classification of a document, but rather to its releasability to anyone, including a visa applicant.

ensure all legal, privacy, civil rights, and civil liberties requirements are satisfied regarding the sharing and use of NIV information in the NVC process. The classified NIV Addendum to the NVC Concept of Operations also contains provisions that govern the scope and protections of information sharing and use.

State has determined that disclosure of NIV data to the NIV Vetting Support Agencies to provide vetting support services is compatible with the purposes for which the data was collected and is authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3)—specifically, the routine uses set forth in the State-39 System of Records Notice. These information sharing agreements and the NIV addendum to the classified NVC Concept of Operations have established the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy protections for the data.

Privacy Risk: There is a risk that the NVC process will result in information being shared with Vetting Support Agencies that do not have authority to support visa vetting activities or do not have data relevant to visa adjudications based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the PCRCL Working Group, supporting the National Vetting Governance Board, are charged with ensuring NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the NVC Implementation Plan and reviewed the NVC's technical designs, plans, and deployment to ensure they meet all legal and PCRCL requirements. These reviews included an evaluation by the working group members, including representatives from the NIV Vetting Support Agencies and State, to ensure that the vetting does not exceed the legal authorities of either State or the NIV Vetting Support Agencies. In addition, agency legal counsel and PCRCL offices at State, DHS, and the NIV Vetting Support Agencies are engaged in reviews of the same issues to ensure their agencies are complying with applicable laws and PCRCL policies, standards, and practices.

Redress

For NIV applicants who were refused visas, no process exists by which the visa refusal can be challenged or reconsidered other than by submitting a new visa application. Consular Officers' determinations may not be overruled, but they are subject to appropriate internal reviews at post by a supervisory Consular Officer or another appropriate official while the visa case is pending. In most cases, the Consular Officer notifies the applicant of the section of law that was determined to be the basis for denial. The Consular Officer may also inform applicants that they may reapply for a visa; a subsequent application is considered a new case. Applicants are generally advised whether they may apply for a waiver of their ineligibility.[107]

State generally applies the protections of the Privacy Act of 1974 (Privacy Act), as amended and codified at 5 U.S.C. § 552a, consistent with its published regulations. But pursuant to sections

[107] Under certain circumstances, such as for humanitarian reasons, an applicant who has been denied a visa may be issued a temporary waiver or pardon of the indelibility to travel (approved by DHS) provided they abide by a pre-defined set of terms.

(k)(1)-(3) of the Privacy Act, it does not make available the accounting of disclosures of a record to the subject of the record where such disclosures would otherwise be required by section (c)(3) of the Privacy Act or permit individuals protected by the Privacy Act to access or review visa records pertaining to them as would otherwise be required by section (d) of the Privacy Act.[108] Further, under State regulations, records exempted by the originator of the record under sections (j) or (k) of the Privacy Act retain their exemptions if subsequently incorporated into any State system of records, provided the reason for the exemption remains valid and necessary.

An NIV applicant may seek to review information about them by following the individual access, redress, and correction procedures described in the State-39 System of Records Notice. If State receives an inquiry about a person that concerns a derogatory entry in the Consular Lookout and Support System database that originated from State, the requestor may be directed to DHS's Traveler Redress Inquiry Program (DHS TRIP).[109] DHS Traveler Redress Inquiry Program will coordinate the review of the requestor's case with the appropriate agency or agencies, which will make any necessary changes to the requester's records.

State and the NIV Vetting Support Agencies will respond to requests for records in accordance with their applicable policies, practices, and procedures, including, but not limited to, responses to requests submitted by Congress, the Government Accountability Office, or members of the public under the Privacy Act, Freedom of Information Act, or Judicial Redress Act of 2015 (5 U.S.C. § 552a note). Any such requests to State for NIV Vetting Support Agency responses provided in response to NIV Vetting Support Requests will be coordinated with those agencies prior to response, and any request for data provided to an NIV Vetting Support Agency will be coordinated by that agency with State prior to response. To the extent permissible under applicable law, the agency receiving the request will defer to the data originator for a determination as to the proper response. If non-attribution for a response provided by an NIV Vetting Support Agency is, in that agency's conclusion, appropriate, State will respond to the request without attribution to the specific NIV Vetting Support Agency, thereby protecting the source of the information from disclosure.

Privacy Risk: There is a risk that individuals will not have the ability to contest a visa adjudication that used information provided through the NVC process and technology as part of the determination.

Mitigation: This risk is mitigated by the ability of a visa applicant to re-apply for a visa. In cases in which a visa applicant believes a visa denial under 8 U.S.C. § 1182(a)(3)(B) is in error or based on incorrect information, they may seek review and correction of that information via the DHS Traveler Redress Inquiry Program process.

Auditing and Accountability

[108] Pursuant to 8 U.S.C. § 1202(f), visa records are generally not releasable under the Freedom of Information Act or the Privacy Act to a first-party requestor unless the document was submitted by or sent to the requesting party.
[109] For more information about DHS TRIP, please see www.dhs.gov/dhs-trip.

The NVC process and technology includes an audit function that captures electronic messages and transactions within its own technology and with other systems involved in the NIV vetting workflow. The audit function logs user activity throughout the vetting workflow to include the original Vetting Support Request, NIV Vetting Support Responses, and State Vetting Analyst recommendations. The format and location of these records enhances metrics reporting, support to redress processes, and records retrieval for compliance and oversight purposes.

Responsible Officials

Monte Hawkins
Director
National Vetting Center
Department of Homeland Security

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
Department of Homeland Security

NVC PIA Addendum 6:

Vetting in Support of the USCIS Asylum Program (UAP)

Last updated February 6, 2024 (back to top)

Under § 208(a) of the Immigration and Nationality Act (INA), as amended and codified at 8 U.S.C. § 1158(a), noncitizens who are physically present or arrive in the United States may apply for asylum. To receive asylum, a noncitizen

[110] must meet the statutory definition of a refugee,[111] be already present in the United States or seeking admission at a port of entry, and merit a favorable exercise of discretion. A noncitizen is barred from receiving asylum, among other reasons established by statute, if they have been convicted of a particularly serious crime or committed a serious non-political crime outside of the United States, if they fall within the INA's inadmissibility or removability grounds relating to terrorism, or if they otherwise pose a threat to national security or public safety. The burden of proof is on the applicant to establish identity and eligibility for asylum.

The authority to adjudicate an application for asylum from noncitizens, who are physically present in the United States and not in removal proceedings, resides with USCIS. This is sometimes referred to as a grant of "affirmative" asylum, and is distinct from "defensive" asylum, in which a noncitizen asserts eligibility for asylum as a form of relief from removal before the Department of Justice's Executive Office for Immigration Review (EOIR). Noncitizens may apply for affirmative asylum regardless of their immigration status through submission of an application (Form I-589, *Application for Asylum and for Withholding of Removal*) with USCIS. The principal applicant may add a spouse or unmarried children under the age of 21 to the application, referred to as "derivative applicants," provided the derivative applicants are also physically present in the United States and not under the jurisdiction of EOIR.[112]

Under an interim final rule effective May 31, 2022, USCIS also has the authority to adjudicate an application for asylum for noncitizens apprehended at the border and in expedited removal proceedings and either retained by USCIS or referred to USCIS by an EOIR immigration judge, via the asylum merits interview (AMI) process.[113] In either case, the applicant must have established a credible fear of persecution or torture as determined by a USCIS Asylum Officer after interviewing the applicant. The written record of a positive credible fear finding, rather than a Form

---

[110] Consistent with DHS policy, the term "noncitizen" is used to throughout this document to describe the individuals defined in 8 U.S.C. § 1101(a)(3) and refers to any person not a national or citizen of the United States.

[111] Under the INA, the term "refugee" refers to the following:

> [A]ny person who is outside any country of such person's nationality or, in the case of a person having no nationality, is outside any country in which such person last habitually resided, and who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.

[112] Even if the applicant does not intend to request asylum for their dependents, they must list their spouse, children, parents, and siblings on their Form I-589 pursuant to USCIS regulation.

[113] Interim Final Rule effective May 31, 2022, *Procedures for Credible Fear Screening and Consideration of Asylum, Withholding of Removal, and CAT Protection Claims by Asylum Officers.* USCIS intends to phase in implementation of the Asylum Merits Interview process, beginning with applicants apprehended at certain Southwest Border sectors or stations and whose final destination is near a USCIS interview office.

I-589, constitutes the asylum application.

The INA and the Homeland Security Act of 2002 authorize USCIS to review and collect additional information concerning asylum applicants to determine their eligibility for asylum status. In doing so, USCIS is separately authorized by the INA to maintain direct and continuous relationships with security partners. USCIS leverages these authorities to conduct both biometric and biographic identity and background checks at multiple stages in the application process. Primarily, these checks are conducted by USCIS against law enforcement, border security, and Department of State (State) data, with results stored in the USCIS Global Information system (Global),[114] USCIS's case management system.

Pursuant to statute and regulation, USCIS Asylum Officers conduct non-adversarial interviews with all affirmative asylum applicants, generally within 45 days from the filing of their Form I-589. The purposes of the interview are to: (1) determine whether the applicants meet the statutory criteria for asylum, including whether they are ineligible due to national security concerns, links to terrorism, criminal history, or other statutory criteria; (2) verify biographic information provided by the applicants; and (3) collect additional biographic information, as appropriate. Prior to the interview, the USCIS Asylum Officer reviews the application and any supporting documentation, including the results of any security checks. The USCIS Asylum Officer uses this review to inform the adjudication of the affirmative asylum application. If the USCIS Asylum Officer identifies any new biographic identifiers during review of the documentation or the interview, this information is added to Global and new security checks will be initiated, if required.

NVC Support to the USCIS Asylum Program (UAP)

The starting point for UAP vetting through the NVC is the transmission of a Vetting Support Request, which consists of applicant information derived from (1) USCIS Form I-589 (for affirmative asylum applicants and unaccompanied noncitizen children), (2) a CBP officers' encounter with the applicant and subsequent asylum merits interview process conducted by a USCIS Asylum Officer, or (3) any electronic applications submitted through USCIS's online portal.[115] UAP Vetting Support Requests may also be enhanced with additional information relating to the individuals found in authoritative data sources already available within CBP's Automated Targeting System (ATS).[116] This process provides additional information for Vetting Support Agencies to match against and allows USCIS to make better informed decisions based on all relevant and appropriate information available to it. The data sources and specific data elements leveraged for vetting record enhancement are agreed upon by CBP as the provider of this technical service, the data originators, the Vetting Support Agencies (VSA), and USCIS as the adjudicating agency.

USCIS Vetting Analysts, possessing the appropriate security clearances, then use the NVC technology to receive and review any relevant and appropriate classified or unclassified information

[114] *See* DHS/USCIS/PIA-027(d) USCIS Asylum Division, *available at* www.dhs.gov/privacy.
[115] After the submission of the initial Vetting Support Request, and during its review of an asylum application, USCIS may identify relevant biographic data from sources other than the Form I-589 or the asylum merits interview, such as from the interview conducted as part of the affirmative asylum process or from visa, travel, or encounter records, or documents presented by the applicant during the interview. If this information differs from the information in the applicant's Form I-589 or asylum merits interview, USCIS may update its systems with the additional data.
[116] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* https://www.dhs.gov/privacy.

made available to them by one or more Vetting Support Agencies. USCIS Vetting Analysts review the information and make a recommendation about whether the applicant(s) may pose a national security, fraud, or public safety concern. The Analyst's recommendation is communicated to a USCIS Asylum Officer, who reviews the recommendation and all other information available to them to adjudicate the asylum claim.

The NVC's process and technology will allow for the:

- Distribution of Vetting Support Requests to UAP Vetting Support Agencies;
- Receipt of Vetting Support Responses from UAP Vetting Support Agencies and distribution to USCIS Vetting Analysts;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for USCIS Vetting Analysts to access classified and unclassified records identified by UAP Vetting Support Agencies as relevant to a Vetting Support Request;
- Support for USCIS Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Managing access to data by individual users and infrastructure according to pre-determined rules and standards;
- Managing the retention of data according to approved record schedules and information sharing agreements;
- Logging user activity for audit, oversight, and accountability purposes; and
- Support for redress processes, Freedom of Information Act (FOIA) requests, discovery in litigation, Congressional inquiries, and other data retrieval requirements.

The NVC leverages the process and technology described in the NVC Privacy Impact Assessment above to facilitate the vetting of UAP applicants, helping to ensure USCIS is informed by all appropriate responsive information held by UAP Vetting Support Agencies.

UAP applicants may adjust to Lawful Permanent Resident (LPR) status following the initial transmission of a Vetting Support Request. USCIS runs daily checks against its holdings to identify when subjects of a UAP vetting request subsequently adjust to Lawful Permanent Resident status. When an individual is identified as having adjusted to Lawful Permanent Resident status, USCIS will initiate a new Vetting Support Request via the NVC with the Lawful Permanent Resident indicator marked as TRUE. That Vetting Support Request will then be transmitted to advise appropriate Vetting Support Agencies of the individual's change in status so they may be handled in accordance with each Vetting Support Agency's authorities, guidelines, policies, and record retention schedules, including their Attorney General-approved guidelines governing the handling of U.S. person information (Attorney General Guidelines).

Privacy Impact Analysis

Authorities and Other Requirements

USCIS's authority to collect information for the administration of the immigration laws and the adjudication of applications for asylum is based upon the Immigration and Nationality Act (INA), 8 U.S.C. § 1101, *et seq.*, including §§ 1103, 1158, 1225, 1228, and 1522. As set forth in Section 451(b) of the Homeland Security Act of 2002, Public Law 107-296 (codified at 6 U.S.C. § 271(b)), Congress charged USCIS with the administration of the asylum program, which provides protection to qualified individuals in the United States who have suffered past persecution or have a well-founded fear of future persecution in their country of origin as outlined under INA § 208 and 8 CFR § 208. USCIS is also responsible for the maintenance and administration of the credible fear and reasonable fear screening processes, in accordance with 8 CFR §§ 208.30 and 208.31.

The following System of Records Notices (SORN) cover the collection, maintenance, and use of information by the USCIS Asylum Division:

- DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records covers the information maintained in the A-File, including hardcopy records of asylum applications, Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203 applications, credible fear screenings, reasonable fear screenings, and supporting documentation.[117]
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records covers the collection, use, and maintenance of asylum applications, NACARA § 203 applications, credible fear screenings, and reasonable fear screenings.[118]
- DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) System of Records governs how USCIS FDNS creates and uses information when reviewing certain applications or individuals for potential fraud, public safety, and national security concerns.[119]
- DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records governs information that is used to verify identity and conduct criminal and national security background checks to establish an individual's eligibility for an immigration benefit or other request.[120]

CBP's Automated Targeting System derives its authority primarily from 8 U.S.C. § 1357; 19 U.S.C. §§ 482, 1461, 1496, and 1581-82; 49 U.S.C. § 44909; the Enhanced Border Security and Visa Reform Act of 2002 (EBSVRA) (Pub. L. 107- 173); the Trade Act of 2002 (Pub. L. 107-210); the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458); and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109-347). Other relevant authorities concerning these activities include 6 U.S.C. §§ 111 and 211; 8 U.S.C. §§ 1103, 1182, 1225- 25a, and 1324; 19 U.S.C. §§ 1431, 1433, 1436, 1448, 1459, 1590, 1594, 1623-24, and

[117] DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[118] DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).
[119] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) System of Records, 77 FR 47411 (Aug. 8, 2012).
[120] DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, 83 FR 36950 (July 31, 2018).

1644-44a.[121]

All activities undertaken through the NVC process are based on existing legal authorities. The use of the NVC process and technology for the UAP program does not provide any new legal authorities to USCIS, CBP, or UAP Vetting Support Agencies to collect, retain, store, or use information, or to make adjudications based on vetting.

Characterization of the Information

The following personally identifiable information may be included in Vetting Support Requests for vetting associated with principal and derivative applicants on an application for asylum:

	Principal Applicant	Derivative Applicant
	X	X
Fingerprint Identification Number (FIN)	X	X
Temporary Protected Status (T or F)	X	X
Full Name	X	X
Gender	X	X
Date of Birth	X	X
Place of Birth	X	X
Passport or National ID	X	X
Telephone Number	X	X
Country of Citizenship	X	X
Country of Residence	X	
Address	X	X
USPER Indicator	X	X
A-Number	X	X
Date of Entry to U.S.	X	X
Status of Entry to U.S.	X	X
Port of Entry to U.S.	X	
Filing Date	X	
Marital Status		X
Relationship to Principal Applicant	X	
Race, Ethnic, Tribal Group	X	
Expiration Date of Travel Document		

[121] DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012).

Privacy Risk: There is a risk that USCIS may make asylum adjudications based on inaccurate information identified during the NVC process.

Mitigation: This risk is partially mitigated. Most of the information used in the NVC process is collected directly from the asylum applicant(s), which should help ensure data accuracy upon collection. However, if an asylum applicant provides inaccurate information, it may result in inaccurate results from the NVC process. Further, some information from USCIS systems and CBP's Automated Targeting System used to enhance asylum vetting records may come from other government data sources. USCIS and CBP rely on those source systems and their data collection processes to ensure that data is accurate and complete. UAP Vetting Support Agencies are required to apply their analytic standards to ensure that information regarding an asylum applicant is objective, timely, relevant, and accurate. For example, UAP Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive 203, which requires that personally identifiable information in analytic products is disseminated "only as it relates to a specific analytic purpose . . . [and] consistent with the [Intelligence Community] element's mission and in compliance with the [Intelligence Community] element's regulation and policy, including procedures to prevent, identify, and correct errors in [personally identifiable information]."[122] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any factors affecting source quality and credibility.[123]

The recommendations provided by USCIS Vetting Analysts inform the ultimate decision regarding an application for asylum. It is the responsibility of the USCIS Asylum Officer to evaluate and assess the totality of the information available to them, including, but not limited to, information provided by UAP Vetting Support Agencies via the NVC process.

Privacy Risk: There is a risk that USCIS Asylum Officers will make adjudications based solely on the Analyst Recommendation.

Mitigation: This risk is mitigated. The goal of the NVC process is to support a recommendation by a USCIS Vetting Analyst based on a consolidated view and analysis of the information made available by the UAP Vetting Support Agencies and all other relevant and available information. The USCIS Asylum Officer will then make an adjudication based on the totality of the information available to them, not only the information provided through the NVC process.

Uses of the Information

USCIS will use the information collected from asylum applicants to analyze potential threats to national security and determine whether the information available raises a question regarding their eligibility to seek asylum under the INA. The additional vetting support provided through the NVC process, supports USCIS's assessment to identify individuals who may pose a risk to national security or public safety when adjudicating applications for asylum.

[122] *See* https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.
[123] *See* https://www.dni.gov/files/documents/ICD/ICD%20206.pdf.

The sharing and use of information made available to USCIS by UAP Vetting Support Agencies is governed by the information sharing agreements in place between those agencies, UAP Vetting Support Agency guidelines, and policies applicable to the sharing of intelligence, law enforcement, or other information. UAP Vetting Support Agencies that are elements of the Intelligence Community must determine that sharing intelligence with USCIS is permitted under their Executive Order 12333 Attorney General-approved Guidelines and other applicable procedures, before they may provide the intelligence information to USCIS through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of asylum applicants' data are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of the data are defined in publicly available documents such as this Privacy Impact Assessment, other relevant Privacy Impact Assessments,[124] System of Records Notices covering the collection of information from USCIS Form I-589,[125] and CBP's Automated Targeting System Privacy Impact Assessment[126] and System of Records Notice.[127] These documents outline the information collected and explain that the information may be shared with other federal departments and agencies for screening and vetting purposes.

Although the NVC process and technology will now be used, the scope of UAP vetting against intelligence, law enforcement, and other information is not changing from the manual processes that occurred previously. Vetting will continue to be defined and governed by existing information sharing agreements and arrangements between USCIS, CBP, and UAP Vetting Support Agencies.

Notice

The I-589 application is accompanied by a Privacy Notice in which it is stated that applicants are submitting their information to DHS/USCIS, that the submission of the information is voluntary, and how that data will be used and shared by DHS/USCIS. The application also provides the authorities under which their information is collected.

Most of the information regarding asylum applicants within CBP's Automated Targeting System is collected directly from the individuals. Additional information regarding asylum applicants within CBP's Automated Targeting System may be derived from other government data sources. Notice for this additional information is provided through the applicable source systems' System of Records Notices and Privacy Impact Assessments (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information.

---

[124] *See* DHS/USCIS/PIA-027 USCIS Asylum Division Privacy Impact Assessment, *available at* www.dhs.gov/privacy.
[125] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017); DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) System of Records, 77 FR 47411 (Aug. 8, 2012).
[126] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[127] DHS/CBP-006 Automated Targeting System (ATS) System of Records, 77 FR 30297 (May 22, 2012).

Privacy Risk: There is a risk that asylum applicants may not be aware and did not knowingly consent to their personally identifiable information being used for vetting purposes.

Mitigation: This risk is partially mitigated. Individuals completing and filing the I-589, *Application For Asylum and for Withholding of Removal,* including unaccompanied children, authorize the release of information contained in the application, supporting documents, and their USCIS records to other entities and persons where necessary for the administration and enforcement of U.S. immigration law. However, certain information stored in CBP's Automated Targeting System may not be directly collected from the asylum applicant. Information within CBP's Automated Targeting System is provided by various government data sources, and notice is provided through the applicable source systems' System of Records Notices and Privacy Impact Assessments (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information.

Data Retention by the Project

USCIS owns and maintains the official record copy of the UAP Vetting Record stored in the NVC technology and retained in accordance with the applicable USCIS records schedule, which mandates a retention period of 100 years from the applicant's date of birth.[128]

Individual Vetting Support Agencies may also maintain internal records reflecting the results of the automated and manual reviews sent to the NVC. Where a Vetting Support Agency has identified and confirmed an analytically significant, also known as "Analytically Significant Threat Information (ASTI)," match related to a vetting request, the Vetting Support Agency may retain that information as authorized by applicable Attorney General-approved Guidelines or as law enforcement information pursuant to the Vetting Support Agency's record control schedules. However, any further disclosure of information retained as analytically significant is only permissible with USCIS approval. In no event shall a Vetting Support Agency retain vetting request information not determined to constitute an analytically significant match for longer than three years (USCIS's approved retention period for this data).

Privacy Risk: There is a risk that Vetting Records created through the NVC process and technology will be retained longer than necessary.

Mitigation: This risk is mitigated. Existing and new information sharing agreements between Adjudicating Agencies and Vetting Support Agencies that define the retention of data are reviewed by the NVC's Legal Working Group and Privacy, Civil Rights, and Civil Liberties (PCRCL) Working Group prior to the on-boarding of any new vetting programs to the NVC process. These information sharing agreements are reviewed with the retention periods outlined in applicable Privacy Impact Assessments, System of Records Notices, record retention schedules, and Attorney General-approved Guidelines. These reviews ensure that retention policies are appropriate and balance the U.S. Government's need to retain the data for operational purposes and afford effective

[128] U.S. National Archives and Records Administration Disposition Authority Number DAA-0563-2013-0001-0005. To calculate the retention period for vetting records within the NVC technology, USCIS will use the date of birth of the subject of the vetting request if one is available. Typically, USCIS will have dates of birth for the primary applicant and any derivative applicants. For records in the NVC technology where there is no date of birth for the subject of the vetting request, USCIS will use the primary applicant's date of birth to calculate the retention period.

redress against the risks to individuals that lengthy retention periods may create (e.g., data breaches and the possible adverse consequences of relying on aging, inaccurate data).

Additionally, the NVC Privacy, Civil Rights, and Civil Liberties Officer is reviewing initiatives underway within DHS to better assess an individual's status and disseminate information when an individual changes status, such as when an individual becomes a U.S. Person. USCIS runs daily checks against its holding to identify individuals that subsequently adjust to Lawful Permanent Resident status. When an individual is identified as having adjusted to Lawful Permanent Resident status, USCIS will initiate a new Vetting Support Request via the NVC with the Lawful Permanent Resident indicator marked as true. Such information sharing is particularly important to remove individuals who have changed status from recurrent vetting in appropriate circumstances.

Information Sharing

Neither National Security Presidential Memorandum (NSPM)-9 nor the NVC provide any new legal authority to USCIS, CBP, or UAP Vetting Support Agencies to collect, retain, store, or use information as part of the UAP vetting mission. All vetting activities for UAP using the NVC process and technology are based on existing legal authorities. Existing external information sharing and access agreements supporting the vetting arrangements have been reviewed by USCIS, CBP, and the Vetting Support Agencies to ensure all legal, privacy, civil rights, and civil liberties requirements are satisfied regarding the sharing and use of UAP information in the NVC process. These information sharing agreements and the classified U A P Addendum to the NVC-Intelligence Community Support Element Concept of Operations have established the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and appropriate privacy, civil rights, and civil liberties safeguards and protections for the data, including special protected class information.

USCIS and CBP have determined that disclosure of their UAP applicant data to the Vetting Support Agencies to provide vetting support services is compatible with the purposes for which the data was originally collected and is authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3) (specifically, the routine uses set forth in the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records; DHS/USCIS-010 Asylum Information and Pre-Screening System of Records; DHS/USCIS-006 Fraud Detection and National Security Records (FDNS); DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records; and DHS/CBP-006 Automated Targeting System).

Privacy Risk: There is a risk that the NVC process will result in information being shared with Vetting Support Agencies that do not have authority to support UAP vetting activities or do not have data relevant to UAP adjudications based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the Privacy, Civil Rights, and Civil Liberties Working Group supporting the National Vetting Governance Board are charged with ensuring NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the NVC Implementation Plan, the classified UAP Addendum to the NVC-Intelligence Community Support Element Concept of Operations, and the NVC's technical designs, plans, and deployment to ensure they meet all legal and privacy, civil rights, and civil liberties requirements. These reviews

included an evaluation by the working group members, which include representatives from various Vetting Support Agencies and DHS, to ensure that the vetting does not exceed the legal authorities of either DHS or the Vetting Support Agencies. In addition, agency legal counsel and privacy, civil rights, and civil liberties offices at DHS and the Vetting Support Agencies are engaged in reviews of the same issues to ensure their agencies are complying with applicable laws and privacy, civil rights, and civil liberties policies, standards, and practices. Information sharing agreements are in place to facilitate information sharing between USCIS, CBP, and UAP Vetting Support Agencies. These agreements have also been reviewed by oversight offices to ensure that all legal and privacy, civil rights, and civil liberties requirements are being fulfilled.

Redress

The NVC does not possess the authority to collect, retain, use, or share information of its own and therefore does not provide any specific redress process. The NVC defers to the process or processes that Adjudicating Agencies employ to provide redress to individuals regarding their adjudications, where applicable.

If NVC vetting results are considered in connection with the negative adjudication of an individual's asylum claim, individuals will receive all process due under the INA.

USCIS and the UAP Vetting Support Agencies will respond to requests for records in accordance with their applicable policies, practices, and procedures, including, but not limited to, responses to requests submitted by Congress, the Government Accountability Office, other oversight entities, or members of the public under the Privacy Act, Freedom of Information Act, or Judicial Redress Act. Any such requests to USCIS for UAP Vetting Support Agency responses provided in response to Vetting Support Requests will be coordinated with those agencies prior to response, and any request for UAP data provided to a Vetting Support Agency as a Vetting Support Request will be coordinated by that agency with USCIS prior to response. To the extent permissible under applicablelaw, the agency receiving the request will defer to the data originator for a determination on the proper response. If non-attribution for a response provided by a UAP Vetting Support Agency is, in that agency's conclusion, appropriate, USCIS will respond to the request without attribution to the UAP Vetting Support Agency, thereby protecting the source of the information from disclosure.

Privacy Risk: There is a risk that individuals will not have the ability to contest the adjudication of an asylum claim that used information provided through the NVC process and technology as part of the determination.

Mitigation: This risk is partially mitigated. If NVC vetting results are considered in connection with a negative adjudication of an asylum claim, individuals will receive all process due under the Immigration and Nationality Act. Further, individuals seeking notification of and access to any records related to USCIS asylum adjudications may submit a request to the USCIS Freedom of Information Act Office at FOIAPAQuestions@uscis.dhs.gov. All or some of the requested information may be exempt from access pursuant to the Privacy Act or the Freedom of Information Act (for those individuals who are not U.S. citizens or Lawful Permanent Residents and whose records are not covered by the Judicial Redress Act) to prevent harm to law enforcement investigations or national security interests.

Auditing and Accountability

The NVC process and technology includes an audit function that captures electronicmessages and transactions within its own technology and with other systems involved in the UAP vetting workflow. It has the capability to allow full review of the actions that occurred in the workflow, beginning with the original Vetting Support Request, through all UAP Vetting Support Responses, to any Analyst Recommendations. The format and location of these records permits the reporting of metrics, support of redress processes, and retrieval of records for compliance and oversight purposes.

Responsible Officials

Daniel P Callahan
Director (A)
National Vetting Center
Department of Homeland Security

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

NVC PIA Addendum 7:

Vetting in Support of State's Immigrant Visa Program (IV)

Last updated May 21, 2024 (back to top)

Under the Immigration and Nationality Act (INA), as amended and codified at Title 8 of the U.S. Code, a noncitizen individual ordinarily requires appropriate documentation, including a visa to travel to the United States and be admitted at a U.S. port of entry. Before issuing a visa, a Department of State (State) consular officer must determine that a noncitizen individual qualifies for the classification of the visa sought and is not inadmissible under the Immigration and Nationality Act or any other provision of U.S. law. The Immigration and Nationality Act sets forth numerous grounds of ineligibility for a visa, including a series of grounds pertaining to criminal-related activity and a separate series of security-related grounds, which includes grounds pertaining to terrorist activities (e.g., 8 U.S.C. § 1182). Ultimately, it is the applicant's burden to establish to that they are eligible to receive a visa.

Immigrant Visas (IV) are issued to foreign nationals seeking to live and work permanently in the United States. To support State's functions in adjudicating visa applications, U.S. law generally requires federal law enforcement agencies and the Intelligence Community (IC) to provide State with information relevant to the determination of a noncitizen's eligibility for a visa (e.g., 8 U.S.C. § § 1105, 1722(a)). For decades, State has leveraged this information to support the review of IV applications and to assist consular officers in determining a visa applicant's eligibility to receive a visa and travel to the United States.

IV Process

Consular officers approve IVs in a number of categories based on family ties, employment, adoption, special immigrant categories, and diversity. The IV process starts with the U.S. Citizenship and Immigration Services (USCIS) approval of an IV petition filed on behalf of the intending immigrant. Upon approval, USCIS transfers the petition to State's National Visa Center for case management within State's systems, including the Consular Electronic Application Center (CEAC).[129]

All IV applicants, including Diversity Visa (DV) applicants, must complete and submit the online Application for Immigrant Visa and Alien Registration Form (DS-260) through State's Consular Electronic Application Center system. State's National Visa Center handles pre-interview processing of IV cases by collecting fees, information, and documentation from applicants, lawyers, and/or sponsors, and then schedules the cases for interviews. In lieu of a USCIS petition, Diversity Visa applicants individually submit entries to State, following applicable rules and regulations.[130]

State's Kentucky Consular Center (KCC) selects entrants and schedules consular interviews once (1) the applicants have submitted DS-260 Forms, (2) the designated post has available appointments, (3) the Kentucky Consular Center has completed processing; and (4) State's visa officer

[129] *See* Consular Electronic Application Center (CEAC) Privacy Impact Assessment, *available at* https://www.state.gov/privacy-impact-assessments-privacy-office/.

[130] Each year, a specific number of IVs are allocated to the Diversity Visa program (a specific subset of the larger IV program), which accepts individual applications from nationals of all countries eligible to participate in the program. Using a random selection process, State identifies applications to proceed to apply for a Diversity Visa.

has allocated visa numbers and the selectee's case is next in the selection order. Once pre-interview processing is complete, the Kentucky Consular Center schedules Diversity Visa cases and the National Visa Center schedules all other IV cases for consular interview. Once scheduled for an interview, all applicants complete certain additional preparations in their home countries and then attend an interview with a consular officer at a U.S. embassy or consulate overseas. Security vetting for all IV applications occurs during consular officer processing of the case. Once the consular officer approves an IV, a visa is placed in the intending immigrant's passport. Issuance of the visa authorizes the applicant to travel to the United States no later than the IV expiration date. An issuance of an IV does not grant admission into the United States; instead, it grants the IV holder authorization to travel to the United States to apply for admission with DHS/U.S. Customs and Border Protection (CBP). If an IV is denied, the consular officer will inform the visa applicant of the denial and the reason for denial.

In addition, consular officers process some Asylee Follow-to-Join (V92) and Refugee Follow-to-Join (V93) cases on behalf of USCIS for beneficiaries of I-730 petitions[131] who are seeking to join asylee or refugee family members in the United States. If approved, the consular officer will issue the applicant a travel document, known as "boarding foils." Boarding foils are not visas, but they are processed through State's IV processing system (or in the non-immigrant visa processing system at non-IV consular sections), and are printed and placed in the applicant's passport, much like a visa.

State Vetting Analysts operate under the authority and control of the Department of State. State Vetting Analysts provide recommendations to consular officers at post, who adjudicate applications in accordance with existing law and policy. State consular officers retain full authority for making all adjudications of visa cases and for all issuances and refusals of visas based on the totality of the information available to them. Designated State Vetting Analysts may be physically or virtually co-located at the NVC, where they will leverage the NVC process and technology. State vetting activities leveraging the NVC process and technology are coordinated with the NVC director.

NVC Support to the IV Process

The NVC leverages the process and technology described in the NVC Privacy Impact Assessment above to facilitate the vetting of IV application data, helping to ensure that State adjudications are informed by all appropriate responsive information held by IV Vetting Support Agencies in a timely and comprehensive manner. The starting point for the vetting of all IV applicants through the NVC process and technology is the transmission of an IV Vetting Support Request, which consists of IV application data, to the IV Vetting Support Agencies.[132] A new information sharing agreement between State, NVC, and Vetting Support Agencies determines which data fields in the application are included in the Vetting Support Request and how they are delivered to Vetting Support Agencies. The NVC facilitates the process through which IV Vetting Support Agencies make available Vetting Support Responses for review by State. State Vetting

[131] A principal refugee admitted to the United States within the past 2 years or a principal asylee who was granted asylum within the past 2 years may request that their spouse and unmarried children under 21 years of age join them in the United States.

[132] As explained in this Privacy Impact Assessment, the NVC does not make recommendations or adjudications. Its role is limited to that of a facilitator or service provider of the NVC process and technology used to facilitate vetting and adjudications by State.

Analysts use NVC technology to receive and review any IV Vetting Support Requests for which there is a relevant classified or unclassified record made available by the IV Vetting Support Agencies. State Vetting Analysts develop a recommendation to either grant or deny the visa based on their analysis of this information in accordance with existing law and policy. State consular officers at post then review the recommendation and any notes provided by the State Vetting Analyst, along with any additional unclassified information available through other appropriate channels, to make their final decision to grant or deny the IV application.

The NVC's process and technology will allow for the:

- Distribution of Vetting Support Requests (i.e., data from all IV applications) to IV Vetting Support Agencies;
- Receipt and distribution of Vetting Support Responses from IV Vetting Support Agencies to State;
- Workflow management of Vetting Support Responses;
- Integrated view-only capability for State Vetting Analysts to access classified and unclassified records identified by Vetting Support Agencies as relevant to a Vetting Support Request;
- Support for State Vetting Analysts to document their analysis and recommendations;
- Storage and correlation of Vetting Support Requests and Vetting Support Responses;
- Management of access to data by individual users and infrastructure according to pre-determined rules and standards;
- Management of the retention of data according to approved IV record schedules and information sharing agreements;
- Logging of user activity for audit, oversight, and accountability purposes; and
- Support for IV redress procedures, Freedom of Information Act (FOIA), 5 U.S.C. § 552, requests, discovery in litigation, Congressional inquiries, and other data retrieval requirements.

DHS/U.S. Immigration and Customs Enforcement (ICE) Support to IV Vetting

As a Vetting Support Agency, ICE will provide support to State by searching for analytically significant threat information (ASTI)[133] found within DHS holdings.

An ICE analyst is tasked with reviewing the application and conducting research within DHS holdings. ICE analysts will use CBP's Unified Passenger (UPAX) to query CBP's Automated

[133] Analytically significant threat information provides analytic insight into the threat posed by an individual or group, whether directly or indirectly, to national security, homeland security, border security, or public safety. Information contained in a Vetting Support Request that is linked to other information available to Vetting Support Agencies through the NVC process only qualifies as analytically significant threat information where the link is accurate and sufficiently analytically significant to warrant dissemination outside of the Vetting Support Agency consistent with the guidelines, processes, and procedures of the Vetting Support Agency identifying the information.

Targeting System (ATS)[134] to access law enforcement, border crossing, and immigration data from various DHS systems, including, but not limited to CBP's TECS[135] and ICE's Enforcement Integrated Database.[136] The ICE analyst may also separately query ICE's Investigative Case Management System (ICM) [137] for further information. ICE analysts will not query any DHS classified information when conducting their research.

Based on an ICE analyst's review, there are two potential outcomes: (1) If the ICE analyst confirms the presence of ASTI in DHS unclassified holdings, they will flag it in Unified Passenger. Unified Passenger will then send a "Reviewed Red" message to the NVC where it can be reviewed by a State Vetting Analyst; (2) If the ICE analyst concludes that there is no ASTI in DHS unclassified holdings, then a "Reviewed Green" message will be sent.

State Vetting Analysts will review responses from all Vetting Support Agencies, including ICE, and begin the State Visa Office's process for making a recommendation on whether to refuse or issue the visa. That recommendation is ultimately sent from the Visa Office to the State consular officer, who has the authority to adjudicate the visa application.

Privacy Impact Analysis

Authorities and Other Requirements

State collects IV application information pursuant to 5 U.S.C. § 301 (Secretary of State's authorities with respect to Management of the Department of State); 22 U.S.C. § 2651a (Organization of the Department of State); 22 U.S.C. § 3921 (Management of the Foreign Service); and 8 U.S.C. §§ 1101-1537 (INA). The creation of the NVC does not provide new legal authorities to State to collect, retain, store, or use information, or to make adjudications based on vetting. All activities undertaken through the NVC process are based on State's existing legal authorities. IV Vetting Support Agencies similarly are engaged in the vetting process pursuant to their own existing legal authorities.

IV case records are maintained in a number of State systems, and their use is described in the System of Records Notice (SORN) for all visa records (State-39).[138] This System of Records Notice covers not only the applications themselves, but also their related forms, biometric information such as photographs, communications within and external to State, internal correspondence and notes related to visa adjudications, and the information regarding applicant family members, employers, and references (including U.S. persons).

Characterization of Information

[134] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* https://www.dhs.gov/privacy.
[135] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* https://www.dhs.gov/privacy.
[136] *See* DHS/ICE/PIA-015 Enforcement Integrated Database, *available at* https://www.dhs.gov/privacy.
[137] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), *available at* https://www.dhs.gov/privacy.
[138] *See* Department of State System of Records Notice – Visa Records, STATE-39, 86 Fed. Reg. 61822 (November 8, 2021).

State will continue to collect the same information from IV applicants through the application process, namely via the DS-260. A subset of the information collected via the DS-260 will make up the structured vetting requests generated by the NVC and sent to Vetting Support Agencies. On behalf of State, the NVC will also append an unstructured text file containing all DS-260 information to the vetting requests when sent to the Vetting Support Agencies.

Importantly, this application information will continue to include a digital photograph of the applicant, which will be utilized for manual identity verification purposes, in the same way it was prior to IV's implementation at the NVC, except that these photographs will now be passed to IV Vetting Support Agencies using the NVC's process and technology. IV Vetting Support Agency analyst reviews are automatically triggered where a selector from an application appears to match to information in a Vetting Support Agency's holdings, just as they were prior to the NVC. A significant part of the analytic review conducted by the analyst is determining whether the apparent match concerns the same individual (i.e., whether the applicant is the same person flagged in the partner's holdings). At times, the biographic information available to the analyst is sufficient to confirm or disqualify the match, but there are occasions where the biographic information is insufficient to make a determination (e.g., there may be more than one individual with the same name and date of birth). Where that occurs and the Vetting Support Agency's previously collected information includes a photograph of the individual whose biographic information matched to one or more biographic selectors in the IV application, the analyst may manually compare the photograph included in the IV application package against the photograph in the Vetting Support Agency's holdings to assist in determining whether the automated match was accurate. At no time does the IV Vetting Support Agency engage in automated one-to-one or one-to-many matching of the biometrics, and the manual comparison of photographic information only occurs where there has already been an automated match of biographic selectors and the photographic comparison would supplement the analyst's review of the available biographic information.

Notably, State consular officers will continue to receive recommendations from State Vetting Analysts, albeit through a new process and technology. Specifically, State Vetting Analysts will now view information related to IV applicants and make recommendations to State consular officers through the NVC process and technology. These recommendations are generated by the State Vetting Analysts who, acting under State authorities, analyze information made available by IV Vetting Support Agencies. The nature and scope of information that is made available by the Vetting Support Agencies is defined by the documentation approved by the National Vetting Governance Board that authorizes this vetting support, which is attached as an addendum to the classified NVC Concept of Operations (CONOP).

Privacy Risk: There is a risk that State consular officers may make decisions to grant or deny a visa application based on inaccurate information identified during the NVC process.

Mitigation: This risk is partially mitigated. Information is collected directly from applicants during the IV application process, ensuring a high level of accuracy upon collection. However, if an IV applicant provides inaccurate information, it may result in inaccurate results from the NVC process. State consular officers have the opportunity during the visa application process to communicate with the applicant and ask questions to resolve potential identity matching issues. Furthermore, IV Vetting Support Agencies are required to apply their analytic standards to

ensure that information regarding the applicant is objective, timely, relevant, and accurate. For example, IV Vetting Support Agencies that are elements of the Intelligence Community must comply with Intelligence Community Directive (ICD) 203, which requires that personally identifiable information is disseminated "only as it relates to a specific analytic purpose . . . [and] consistent with IC element mission and in compliance with IC element regulation and policy, including procedures to prevent, identify, and correct errors in [personally identifiable information]."[139] Consistent with Intelligence Community Directive 206, intelligence analytic products also should describe any factors affecting source quality and credibility.[140]

The recommendations provided by the State Vetting Analysts inform, but do not determine the outcome of a visa adjudication. It is the responsibility of State's consular officers to evaluate the substance and assessed reliability of the additional information provided by IV Vetting Support Agencies in conjunction with other information available to them when determining whether to approve or deny an IV application.

Privacy Risk: There is a risk that State consular officers will make IV adjudications based solely on the State Vetting Analyst recommendation without considering all appropriate information available to them.

Mitigation: This risk is mitigated. The purpose of the NVC process is not to make an adjudication for State, but rather to facilitate a recommendation from State Vetting Analysts based on a consolidated view and analysis of the Vetting Support Responses and information made available by the IV Vetting Support Agencies. State consular officers will base their adjudications on the totality of the information available to them, including classified and unclassified vetting processes, document reviews, and applicant interviews.

State Vetting Analysts will make their recommendations based on whether the information provided by IV Vetting Support Agencies meets the legal standard described in relevant sections of U.S. law—usually, the grounds of inadmissibility contained in Section 212 of the Immigration and Nationality Act, 8 U.S.C. § 1182. In cases in which the State consular officer believes that a vetting analyst's recommendation of refusal is inconsistent with the totality of available information about the visa applicant, the officer can request a supplementary analysis of the ASTI in the context of all known facts. Ultimately, the decision to grant or deny a visa rests entirely with the State consular officer.

Uses of the Information

State will continue to use the information included in an individual's visa application to determine the eligibility of the foreign national to travel to the United States, including whether the visitor poses a law enforcement or security risk. With the addition of the vetting support provided through the NVC process, State will be better equipped to identify travelers of interest, thereby improving its security capabilities while also facilitating the travel of lawful visitors.

State will continue to employ unclassified vetting processes, document reviews, and

[139] *See* https://www.dni.gov/files/documents/ICD/ICD-203_TA_Analytic_Standards_21_Dec_2022.pdf.
[140] *See* https://www.dni.gov/files/documents/ICD/ICD-206.pdf.

applicant interviews in addition to the vetting facilitated through the NVC process and technology. The addition of the State Vetting Analyst recommendation for State consular officers enhances State's ability to mitigate security gaps.

The sharing and use of information made available to State by IV Vetting Support Agencies is governed by the information sharing agreements in place between those agencies, the classified NVC/Intelligence Community Support Element Concept of Operations, and IV Vetting Support Agency-specific guidelines and policies applicable to the sharing of intelligence, law enforcement, or other information. IV Vetting Support Agencies that are elements of the IC must determine that sharing intelligence with State is permitted under their Attorney General Guidelines for the protection of U.S. person (USPER) information, which are mandated by Executive Order 12333, and other applicable procedures, before they may provide it to State through the NVC process and technology.

Privacy Risk: There is a risk that the stated purposes of the collection of IV data during the application process are inconsistent with the vetting activities that will be facilitated through the NVC process and technology.

Mitigation: This risk is mitigated. The purposes for collection of IV application data, as documented in System of Records Notices, Privacy Impact Assessments, Privacy Act Statements or Privacy Notices, and information sharing agreements, are reviewed as a part of the NVC process to on-board a new vetting program to ensure accuracy and adequate support of vetting activities. This helps to ensure that individuals who provide the information receive adequate public notice of the purposes for which the data is collected and how it is used.

Further, 8 U.S.C. § 1202(f) and interagency information sharing agreements limit the use of data beyond what is authorized and appropriate. Visa records and records containing information subject to 8 U.S.C. § 1202(f) are marked with a prominent banner for notice purposes. Any uses of information protected under 8 U.S.C. § 1202(f) that are not previously authorized under existing agreements require prior approval by State. There will also be prominent banners notifying Vetting Analysts and partners when an individual is protected under the provisions of 8 U.S.C. § 1367. Additionally, Refugee and Asylee Follow-to-Join vetting records, as described above, will be appropriately bannered to reflect the protections under the provisions of 8 C.F.R. § 208.6.

Notice

Individuals who complete an IV application do so after having the opportunity to review the Privacy Notice. They are notified in writing that they are submitting the information to State, how that data will be used/shared, and the authorities under which it is collected.

Privacy Risk: There is a risk that USPER information will be included in the vetting process.

Mitigation: This risk is partially mitigated. The majority of individuals applying for an IV are not USPERs. The key exception to this is individuals requesting an SB-1 IV seeking a visa based on

their putative status as a lawful permanent resident.[141] State will not transmit SB-1 data to the NVC for vetting purposes.

Additionally, while structured vetting requests transmitted via the NVC do not include information about individuals who could potentially be USPERs (petitioner, U.S.-based attorney, third-party agent), Department of State does transmit all data provided via the DS-260 as an unstructured attachment to IV Vetting Support Requests. IV Vetting Support Agencies do not automatically correlate this unstructured data against their holdings, but it may be used during the manual review process, where permissible under a Vetting Support Agency's Attorney General-approved Guidelines.

Privacy Risk: There is a risk that individuals whose information may be included in an IV vetting record (e.g., sponsors, attorney/agent, relatives, petitioners) may not be aware of and did not consent to their information being used for vetting purposes.

Mitigation: This risk is not mitigated. There are some individuals who have a role in the visa application process and others with no role in the visa process but whose information is provided by the applicant that may not be aware of the application or that their information has been provided to the U.S. Government. Accordingly, State and DHS have taken a number of steps to provide general public notice of this fact, including publicly publishing this Privacy Impact Assessment, the State Enterprise Visa Application Forms (EVAF) Privacy Impact Assessment, the State Visa Records System of Records Notice, and privacy notices at State data collection points.

Individuals who have reason to believe that State, the NVC, or Vetting Support Agencies have visa vetting records pertaining to them should follow the instructions under the Notification Procedures and Record Access Procedures sections of the applicable System of Records Notice (e.g., State-39).

Data Retention by the Project

As reflected in the State-39 System of Records Notice, the retention period for IV applications depends on the nature of the information and the disposition of the visa adjudication; however, all IV application data is retained in State systems for 25 years for issued IVs and either 25 or 100 years for refused IVs depending on the grounds for refusal. All State records pertaining to the issuance or refusal of visas, including IV case records, are protected as confidential pursuant to 8 U.S.C. § 1202(f), but this statute permits the limited use of visa records for, among other purposes, the enforcement and administration of the Immigration and Nationality Act and other laws of the United States.[142]

Copies of IV records stored by the NVC on behalf of State are retained for 11 years to satisfy any legal obligations related to litigation, redress, or Freedom of Information Act requests. At all times, IV records are maintained, used, and shared consistent with the provisions of the State-39

[141] A lawful permanent resident or conditional resident who has remained outside the United States for longer than one year, or beyond the validity period of a Re-entry Permit, will require the issuance of an SB-1 immigrant visa to re-enter the United States and resume permanent residence.
[142] As used in this context, the designation "confidential" does not relate to the security classification of a document, but rather to its releasability to anyone, including a visa applicant.

System of Records Notice, as appropriate.

Individual IV Vetting Support Agencies may also maintain internal records reflecting the results of the automated and manual reviews sent forward to NVC Services. Retention periods for any such records are determined by the applicable records schedules for those agencies in accordance with existing information sharing agreements and respective Attorney General Guidelines.

Privacy Risk: There is a risk that IV Vetting Support Agencies will retain information from Vetting Support Requests for longer than is necessary.

Mitigation: This risk is mitigated. State and the IV Vetting Support Agencies reviewed the applicable information sharing agreements that define the retention of data, in coordination with the NVC's Legal Working Group and Privacy, Civil Rights, and Civil Liberties Working Group, prior to the on-boarding of IV vetting into the NVC process. These information sharing agreements were reviewed along with retention periods outlined in applicable Privacy Impact Assessments, System of Records Notices, record retention schedules, and Attorney General Guidelines. These reviews ensured retention policies are appropriate and balance the U.S. Government's need to retain the data for operational purposes and afford effective redress against the risks to individuals that lengthy retention periods may create (e.g., data breaches and the possible adverse consequences of relying on aging, inaccurate data). Additionally, the retention period for IV vetting support records is documented internally in classified documents that outline their specific processes. This documentation defines the authorized retention period of Vetting Support Requests shared with IV Vetting Support Agencies and the purposes for such sharing. IV Vetting Support Agencies may retain vetting records for longer periods when, for example, they are identified as foreign intelligence or are relevant to law enforcement investigations in accordance with existing information sharing agreements, applicable law, and policy. For Vetting Support Request information ingested by IV Vetting Support Agencies' internal systems, this risk is mitigated solely by NVC technologies. This risk is instead mitigated by the internal retention controls of the IV Vetting Support Agencies, including records retention schedules, the National Security Act of 1947, and retention limitations derived from the Agencies' 12333 Attorney General Guidelines.

Information Sharing

Neither National Security Presidential Memorandum-9 nor the NVC provide new legal authority to State or IV Vetting Support Agencies to collect, retain, store, or use IV information. All vetting activities for IV using the NVC process and technology are based on existing legal authorities. State will continue to share IV information in bulk with other federal counterterrorism partners. Existing external information sharing and access agreements supporting these vetting arrangements have been reviewed by State and the IV Vetting Support Agencies to ensure all legal, privacy, civil rights, and civil liberties requirements are satisfied regarding the sharing and use of IV information in the NVC process. The classified IV Addendum to the NVC Concept of Operations also contains provisions that govern the scope and protections of information sharing and use.

State generally applies the protections of the Privacy Act of 1974 (Privacy Act), as amended and codified at 5 U.S.C. § 552a, consistent with its published regulations. But pursuant to sections

(k)(1)-(3) of the Act, it does not make available the accounting of disclosures of a record to the subject of the record where such disclosures would otherwise be required by section (c)(3) of the Act or permit individuals protected by the Act to access or review visa records pertaining to them as would otherwise be required by section (d) of the Act.[143] Further, under State regulation, records exempted by the originator of the record under sections (j) or (k) of the Act retain their exemptions if subsequently incorporated into any state system of records provided the reason for the exemption remains valid and necessary.

Privacy Risk: There is a risk that the NVC process will result in information being shared with IV Vetting Support Agencies that do not have authority to support visa vetting activities or do not have data relevant to visa adjudications based on applicable legal standards.

Mitigation: This risk is mitigated. The NVC Legal Working Group and the Privacy, Civil Rights, and Civil Liberties Working Group, supporting the National Vetting Governance Board, are charged with ensuring NVC activities comply with applicable law and appropriately protect individuals' privacy, civil rights, and civil liberties. The working groups conducted a thorough review of the technical designs, plans, and deployment of IV vetting into the NVC process to ensure that all legal and PCRCL requirements were met. These reviews included an evaluation by the working group members, including representatives from the IV Vetting Support Agencies and State, to ensure that the vetting does not exceed the legal authorities of either State or the IV Vetting Support Agencies. In addition, agency legal counsel and PCRCL offices at State and the IV Vetting Support Agencies engage in similar initial reviews of the same issues to ensure their agencies are complying with applicable laws and PCRCL policies, standards, and practices.

Redress

For IV applicants who were refused visas, no process exists by which the visa refusal can be challenged or reconsidered other than by submitting a new visa application. Consular officers' determinations may not be overruled, but they are subject to appropriate internal reviews at post by a supervisory consular officer or another appropriate official while the visa case is pending. In most cases, the consular officer notifies the applicant of the section of law that was determined to be the basis for denial. The consular officer may also inform applicants that they may reapply for a visa; a subsequent application is considered a new case. Applicants are generally advised whether they may apply for a waiver of their ineligibility.[144]

State generally applies the protections of the Privacy Act, consistent with its published regulations. But pursuant to sections (k)(1)-(3) of the Privacy Act, it does not make available the accounting of disclosures of a record to the subject of the record where such disclosures would otherwise be required by section (c)(3) of the Privacy Act or permit individuals protected by the Privacy Act to access or review visa records pertaining to them as would otherwise be required by

[143] Pursuant to 8 U.S.C. § 1202(f), visa records are generally not releasable under the Freedom of Information Act, 5 U.S.C. § 552, or the Privacy Act to a first party requested unless the document was submitted by the requesting party.
[144] Under certain circumstances, such as for humanitarian reasons, an applicant who has been denied a visa may be issued a temporary waiver or pardon of the indelibility to travel (approved by DHS) provided they abide by a pre-defined set of terms.

section (d) of the Privacy Act.[145] Further, under State regulations, records exempted by the originator of the record under sections (j) or (k) of the Privacy Act retain their exemptions if subsequently incorporated into any State system of records, provided the reason for the exemption remains valid and necessary.

An IV applicant may seek to review information about them by following the individual access, redress, and correction procedures described in the State-39 System of Records Notice. If State receives an inquiry about a person that concerns a derogatory entry in the Consular Lookout and Support System database that originated from State, the requestor may be directed to DHS's Traveler Redress Inquiry Program (DHS TRIP).[146] DHS TRIP will coordinate the review of the requestor's case with the appropriate agency or agencies, which will make any necessary changes to the requester's records.

State and the IV Vetting Support Agencies will respond to requests for records in accordance with their applicable policies, practices, and procedures, including, but not limited to, responses to requests submitted by Congress, the Government Accountability Office, or members of the public under the Privacy Act, Freedom of Information Act, or Judicial Redress Act of 2015 (5 U.S.C. § 552a note). Any such requests to State for IV Vetting Support Agency responses provided in response to IV Vetting Support Requests will be coordinated with those agencies prior to response, and any request for data provided to an IV Vetting Support Agency will be coordinated by that agency with State prior to response. To the extent permissible under applicable law, the agency receiving the request will defer to the data originator for a determination as to the proper response. If non-attribution for a response provided by an IV Vetting Support Agency is, in that agency's conclusion, appropriate, State will respond to the request without attribution to the specific IV Vetting Support Agency, thereby protecting the source of the information from disclosure.

Privacy Risk: There is a risk that individuals will not have the ability to contest a visa adjudication that used information provided through the NVC process and technology as part of the determination.

Mitigation: This risk is partially mitigated. Every visa applicant may re-apply for a visa. No process exists by which the visa refusal can be challenged or reconsidered other than by submitting a new visa application. Consular officers' determinations may not be overruled, but they are subject to appropriate internal reviews at post by a supervisory consular officer or another appropriate official while the visa case is pending. In most cases, the consular officer notifies the applicant of the section of law that was determined to be the basis for denial. The consular officer may also inform applicants that they may reapply for a visa; a subsequent application is considered a new case. Applicants are generally advised whether they may apply for a waiver of their ineligibility.

Privacy Risk: There is a risk that IV applicants may gain USPER status yet not be removed from recurrent NVC vetting in a timely manner.

Mitigation: This risk is mitigated. Certain IV Vetting Support Agencies provide recurrent vetting support of IV applicants from the time they submit their DS-260 to State until the applicant

[145] Pursuant to 8 U.S.C. § 1202(f), visa records are generally not releasable under the Freedom of Information Act or the Privacy Act to a requestor unless the document was submitted by or sent to the requesting party.
[146] For more information about DHS TRIP, please *see* www.dhs.gov/dhs-trip.

arrives at a U.S. port of entry and is admitted by CBP. Upon admission, the individual becomes a lawful permanent resident (i.e., USPER). After the individual is admitted to the United States, the NVC will receive an automated notification from CBP identifying that individual as a USPER. That notification then automatically triggers a notification to the Vetting Support Agencies from the NVC to promptly remove them from recurrent vetting.

Auditing and Accountability

The NVC process and technology includes an audit function that captures electronic messages and transactions within its own technology and with other systems involved in the IV vetting workflow. The audit function logs user activity throughout the vetting workflow to include the original IV Vetting Support Request, IV Vetting Support Responses, and State Vetting Analyst recommendations. The format and location of these records enhances metrics reporting, support to redress processes, and records retrieval for compliance and oversight purposes.

Responsible Officials

Daniel P. Callahan
Acting Director
National Vetting Center
Department of Homeland Security

Approval Signature

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

Mason C. Clutter
Chief Privacy Officer
Department of Homeland Security