Privacy Impact Assessment
for the

National Vetting Center (NVC)

DHS/ALL/PIA-072

December 11, 2018

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.

Overview

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

[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 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.

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 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)

[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.
[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.

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 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 include links or pointers to information that the Vetting Support Agencies believe are valid and analytically significant identity matches, but not the underlying information

[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.*
[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.

itself.[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 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

---

[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.

[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.

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;
- 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

[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.

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 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

[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.

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 being built-out by DHS's Office of Intelligence & Analysis (DHS I&A) is being granted concurrently with the completion of this PIA, along with other compliance requirements.

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 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. Vetting Support Responses also contain links or pointers to any information that the Vetting Support Agencies believe are valid, analytically significant identity matches, but not the underlying information itself. 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

[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.

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 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

[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.
[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.

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 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]

[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.

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 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

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

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

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 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.

---

[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.

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 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**

NVC PIA Addendum 1:

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

Last updated December 11, 2018 (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.

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]

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

[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 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.

(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 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.

---

[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.

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 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

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

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

Approval Signature

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

Philip S. Kaplan
Chief Privacy Officer
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).