Privacy Compliance Review of the U.S. Customs and Border Protection Electronic System for Travel Authorization

October 27, 2017

Contact Point

Todd C. Owen
Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

John Wagner
Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

Reviewing Official

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

I. Background

The Department of Homeland Security (DHS) Privacy Office (PRIV) recently conducted a Privacy Compliance Review (PCR)[1] of the use of social media identifiers[2] by U.S. Customs and Border Protection (CBP) for the vetting of Electronic System for Travel Authorization (ESTA) applications, as required by the September 2016 update to the ESTA Privacy Impact Assessment (DHS/CBP/PIA-007(g)).[3] In September of 2016, CBP began collecting, on a voluntary basis, social media identifiers from citizens and nationals of countries participating in the Visa Waiver Program (VWP)[4] who sought to travel to the United States. ESTA is a web-based application and vetting system used by CBP to determine the eligibility of foreign nationals seeking to travel to the United States under the VWP. Citizens and nationals of VWP countries use the ESTA website[5] to submit biographic information and respond to eligibility-related questions. Through the evolution of the ESTA Program, Privacy Impact Assessments[6] have been conducted in order to document changes to the program, including the optional provision of social media identifiers through the ESTA application, which was approved by the DHS Chief Privacy Officer on September 1, 2016. The inclusion of social media identifiers on the ESTA application is the first time DHS has requested social media information as part of an application for benefits or travel to the United States.

Although the provision of social media identifiers as part of the ESTA application may be optional for the VWP, any information submitted may be used for national security and law enforcement purposes as defined in the ESTA Privacy Impact Assessment (PIA) or ESTA System of Records Notice (SORN).[7]

While providing social media identifiers is optional, should an applicant choose not to voluntarily provide social media information as part of his/her application, DHS/CBP may employ tools and search techniques in an attempt to locate and identify public social media accounts and profiles belonging to the applicant, for use in the screening and vetting process. The PIA discusses this process in detail.

---

[1] The DHS Privacy Office conducts PCRs pursuant to its authority under Section 222 of the Homeland Security Act to assure that technologies sustain and do not erode privacy protections. Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.

[2] As described in the ESTA application, social media identifiers include the username, handle, screen-name, or other identifying information associated with an individual's social media profile.

[3] *See:* DHS/CBP/PIA-007(g) Privacy Impact Assessment Update for the Electronic System for Travel Authorization (September 1, 2016), *available at:* https://www.dhs.gov/publication/electronic-system-travel-authorization.

[4] *See:* 8 CFR § 217. The VWP, administered by DHS in consultation with the U.S. Department of State, permits citizens of 38 countries to travel to the United States for business or tourism for stays of up to 90 days without a visa.

[5] *See*: ESTA Application website *available at*: https://esta.cbp.dhs.gov/esta/.

[6] *See:* all CBP ESTA PIAs *available at*: https://www.dhs.gov/publication/electronic-system-travel-authorization.

[7] *See:* DHS/CBP-009 - Electronic System for Travel Authorization (ESTA) *available at:* https://www.regulations.gov/document?D=DHS-2016-0054-0001.

This report sets forth PRIV's findings and provides recommendations for best practices to protect privacy when collecting and using social media identifiers and to promote compliance with the ESTA PIA.

II. Scope and Methodology

The DHS Privacy Office conducted this PCR to verify that the use of voluntarily provided social media identifiers as part of the ESTA application is in accordance with the conditions outlined in DHS/CBP/PIA-007(g). To achieve that objective, PRIV reviewed existing privacy compliance documentation; developed and submitted an extensive questionnaire designed to build a comprehensive understanding of the vetting process employed under ESTA to the CBP Privacy and Diversity Office (PDO); reviewed CBP responses to said questionnaire, including all supporting documentation; and received briefings and demonstrations from CBP subject matter experts.

The DHS Privacy Office conducted this PCR in coordination with personnel from CBP PDO, the CBP's ESTA program office, and CBP's National Targeting Center (NTC). The findings detailed in this report reflect conclusions reached by the DHS Privacy Office based on an assessment of ESTA-related compliance documentation, exchanges with CBP personnel, and an analysis of documents, responses, discussions, and other information received in response to the initiation of this PCR in May 2017. The report is organized according to the relevant DHS Fair Information Practice Principles[8] (FIPPs).

In conducting this PCR, the DHS Privacy Office:

- Reviewed each of the ESTA Program PIAs, with specific attention paid to DHS/CBP/PIA-007(g);
- Developed and distributed an initial questionnaire covering December 2016 – May 2017 (May 2017);
- Reviewed initial CBP responses and supporting documentation;
- Met with the CBP Branch Chief for Privacy Oversight, the Director of the ESTA Program, and senior personnel from the NTC (May 2017);
- Conducted a site visit at the NTC (June 2017)
- Reviewed CBP's responses to initial PCR questionnaire (July 2017)
- Developed follow-up questionnaires and conducted additional discussions with CBP personnel to better understand responses (July 2017)
- Drafted an initial PCR Report for CBP comments (September 2017);
- Responded to CBP comments (October 2017); and
- Drafted and published final PCR Report (October 2017).

[8] *See:* Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

III. Findings

Summary
The DHS Privacy Office commends CBP for implementing robust privacy protections to strengthen and enhance privacy in the context of the program's collection and use of social media information. The DHS Privacy Office has provided the recommendations below to help guide CBP in further enhancement of best practices to continue to protect privacy, foster adherence to the FIPPs, and promote compliance with the ESTA PIA. The DHS Privacy Office finds the CBP ESTA program's use of social media identifiers is compliant with the requirements outlined in the PIA. Based on our findings, this PCR makes the following recommendations:

> *Recommendation 1:* As a best practice, CBP should make it easier to navigate from the ESTA application webpage to the page where questions related to the collection and use of social media information are addressed.
>
> *Recommendation 2:* CBP should implement a process or mechanism for tracking and measuring the viability and success of the collection and use of social media information as part of the screening and vetting process.
>
> *Recommendation 3:* As a best practice, the ESTA Program should consider developing and providing more clear instructions to applicants aimed at reducing the inaccurate inclusion of non-identifier information in the social media 'free-text' portion of the online application.

Below is a discussion of each FIPP requirement, how the DHS Privacy Office reviewed the program for compliance, our findings, and when necessary, specific recommendations to CBP in response to these findings.

A. Transparency:

Requirement: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

Review: The DHS Privacy Office reviewed the publicly available privacy documentation associated with the ESTA program, including multiple evolutions of the PIA, the SORN, and Privacy Notices associated with the online ESTA application, and CBP's responses to the PCR questionnaire. PRIV also reviewed the online ESTA application, as well as the Help and Frequently Asked Questions (FAQ) pages accompanying it.

Finding: As outlined in *DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable*

Information,[9] DHS treats all persons, regardless of immigration status, consistent with the FIPPs and applicable law. Per the FIPPs framework, the Department must provide transparency for how it handles PII through various mechanisms, including PIAs, SORNs, Privacy Notices, general notices, the conduct of Privacy Compliance Reviews, and the Freedom of Information Act (FOIA). CBP employs each of these instruments in order to operate the ESTA program as transparently as possible.

Transparency of the CBP ESTA program is a prime example for other DHS components, as well as agencies within the Federal Government, with regard to properly managing the transparent collection and use of social media information. CBP provides substantial notice of its use of social media information, including that its provision by ESTA applicants is voluntary and will be used in support of screening and vetting efforts, as part of the determination regarding eligibility to travel to the United States. CBP provides substantial notice to ESTA applicants of the collection, use, dissemination, and maintenance of PII through a variety of publicly available compliance documents, including PIAs and SORNs. CBP provides regular updates to its PIA and SORN, available on the public-facing DHS Privacy Office website, including three separate updates to each document between February and September 2016, to ensure a transparent explanation of the program's use of collected information is provided to the public.

Each of the public resources indicates that the provision of social media identifiers is optional, and extensively details the use of information collected as part of the ESTA application to conduct screening, vetting, and law enforcement checks of ESTA applicants. Furthermore, the public resources note that social media information specifically may be used to support or corroborate a traveler's application information, which will assist in facilitating legitimate travel by providing an additional method of adjudicating possible concerns related to questions about identity, occupation, previous travel, and other factors. In addition, social media may also identify potential deception or fraud. Within the application, CBP provides heading notes and 'pop-up' bubbles reaffirming that the provision of social media identifiers is optional, and outlining what information is being requested.

Also provided on the ESTA application website is a Privacy Notice that elaborates on the information being collected and how it will be used. Though CBP does provide a *Help/Frequently Asked Questions (FAQ)* page within the application website,[10] PRIV did find that it failed to address potential questions and concerns that applicants may have regarding the collection of social media information. Social media-specific information was available, however, through the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act Frequently Asked Questions (FAQ)* webpage.[11]

---

[9] *See:* DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at 3 (April 27, 2017), *available at:* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[10] *See:* ESTA Application: Frequently Asked Questions, *available at:* https://esta.cbp.dhs.gov/esta/application.html?execution=e3s1.

[11] *See:* ESTA Application: Frequently Asked Questions, *available at:* https://www.cbp.gov/travel/international-visitors/visa-waiver-program/visa-waiver-program-improvement-and-terrorist-travel-prevention-act-faq.

Recommendation 1: CBP should make it easier to navigate from the ESTA application webpage to the page where questions related to the collection and use of social media information is addressed.

As evidence of the collaborative format that the PCR process adopts, PRIV identified this recommendation in the course of our review during in-person discussions with the ESTA staff and CBP PDO personnel, and it was remedied prior to the conclusion of this review. In further demonstration of CBP's responsiveness and willingness to cooperate with the DHS Privacy Office in support of this PCR effort, the ESTA team added the same social media-specific language found in the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act Frequently Asked Questions (FAQ)* webpage,[12] to the ESTA application *Help/Frequently Asked Questions (FAQ)* page,[13] making it easier for individuals to locate the information directly from the application.

B. Individual Participation:

Requirement: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Review: PRIV reviewed the online ESTA application and questionnaire responses, conducted personnel interviews, and conducted a site visit at the NTC in order to verify information collection processes. As part of the questionnaire, the DHS Privacy Office requested that CBP provide detailed information related to the participation rates of ESTA applicants in the provision of social media identifiers. Additionally, PRIV requested information on all FOIA requests related to the ESTA program since December 20, 2016, when the collection of social media identifiers began.

Finding: DHS Privacy Policy Guidance Memorandum 2017-01[14] requires that the Department involve the individual in the use of his/her PII, and where possible, seek the person's consent for its collection, use, dissemination, or maintenance. The ESTA program's collection of information through an online application inherently involves the participation of individuals, and by default their consent for the collection and use of the PII that they provide.

---

[12] *See:* ESTA Application: Frequently Asked Questions, *available at:* https://www.cbp.gov/travel/international-visitors/visa-waiver-program/visa-waiver-program-improvement-and-terrorist-travel-prevention-act-faq.
[13] *See:* ESTA Application: Frequently Asked Questions, *available at*: https://esta.cbp.dhs.gov/esta/application.html?execution=e3s1.
[14] *See:* DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at 3 (April 27, 2017), *available at:* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

Additionally, the applicants are required to provide an acknowledgement that they understand three separate notices prior to being provided with the ability to enter information into the application. Upon accessing the ESTA application website, users are required to confirm their understanding of a Security Notification. The notification indicates that applicants are accessing a DHS computer system, the use of which comes with no expectation of privacy, and clearly states that through accessing the system, all users consent to the terms as outlined. A second disclaimer denotes that information entered into the ESTA application will be used to perform checks against law enforcement databases. It also provides information on the ESTA process, and what an individual should expect following an application approval or denial. The applicant must acknowledge that they have read and understand the terms of this disclaimer in order to view the final notice. A Travel Promotion Act of 2009 disclaimer provides notice to applicants that a fee is required for the use of the ESTA system, and the application will not be processed until all payment information is completed. Should an applicant indicate that he or she does not understand either the second or third notification, CBP provides additional information for further clarification via pop-up windows on the website. With regard to social media information, notices on each of the free text fields in which information is input also indicate that the provision of social media identifiers is completely voluntary. During the course of this PCR, 614,077 (approximately 8 percent) of the 7,608,464 applications that were submitted between December 20, 2016, and June 21, 2017, included voluntarily provided identifiers.

In terms of correcting information within the application, individuals are able to correct mistakes in the information that they provide any time before submission. After submission, applicants may correct errors in data fields other than biographical and passport information through the *"Check Individual Status"* section of the application website. If an applicant made a mistake on his or her passport or biographical information, he or she may submit a new application. With regard to additional redress, individuals seeking access to any record held by DHS containing personal information may submit FOIA requests. Applicants from certain foreign nations may be able to request access and amendment to records in accordance with the Judicial Redress Act,[15] which provides them with protections similar to those afforded by the Privacy Act of 1974, as amended.[16] During the period of this review, CBP received only one FOIA request related to the ESTA program. While this pertained to a request for an individual's travel record and not necessarily information specific to the ESTA application, CBP demonstrated that a process is in place for applicants to seek access and redress.

PRIV also finds that CBP's use of social media information under the ESTA program is in line with the individual participation provisions of the *Department's Privacy Policy for the Operational Use of Social Media*.[17] The instruction provides guidance to Department personnel

[15] *See:* Public Law 114-126, 130 Stat. 282 (February 24, 2016), *available at:* https://www.gpo.gov/fdsys/pkg/BILLS-114hr1428enr/pdf/BILLS-114hr1428enr.pdf.

[16] *See:* 5 U.S.C. § 552a, *available at:* https://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf.

[17] *See:* DHS Instruction Number: 110-01-001 – Privacy Policy for Operational use of Social Media, *available at:* https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.

regarding access to, and the collection, use, maintenance, retention, disclosure, deletion, and destruction of PII through the operational use of social media. As required by the Rules of Behavior portion of the instruction, CBP officers and analysts supporting the ESTA screening and vetting effort only access social media information that is publicly available, respecting the individual's privacy settings. By limiting the use of information to only that which is publicly available, CBP is only assessing statements and postings that the applicant chose to share publicly.

C. Purpose Specification:

Requirement: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Review: The DHS Privacy Office reviewed the Privacy Notice posted on the ESTA application website, which cites the program's authority to collect information, as well as the purpose for the collection, the ways in which that data is shared, and any consequences an individual may face for not providing necessary information. Additionally, PRIV reviewed the September 2016 update to the ESTA Privacy Impact Assessment (DHS/CBP/PIA-007(g))[18] and other applicable compliance documentation, including Privacy Threshold Analyses and Social Media Operational Use Templates (SMOUT), to gain a complete understanding of the use of information collected within the ESTA application, specifically social media identifiers. PRIV's understanding of how ESTA data is used was confirmed through discussions with personnel from the program, the NTC, and CBP PDO.

Finding: CBP is operating in accordance with its authorities to collect information in support of the screening and vetting of ESTA applications.[19] Social media identifiers provided by applicants are used to conduct screening, vetting, and law enforcement checks in order to make eligibility determinations for individuals from VWP countries seeking to travel to the United States. Social media information, whether provided by an ESTA applicant or located by officers and analysts during the adjudication process, is used to assist in determining the individual's eligibility to travel to the United States under VWP, to assist in determining if the applicant poses a law enforcement or security risk, as well as mitigate potentially derogatory information that would likely have resulted in the denial of the individual's ESTA application. ESTA and NTC

[18] *See:* DHS/CBP/PIA-007(g) Privacy Impact Assessment Update for the Electronic System for Travel Authorization (September 1, 2016), *available at:* https://www.dhs.gov/publication/electronic-system-travel-authorization.

[19] Collection of the information solicited in the ESTA application is authorized by Title 8 of the United States Code. Specifically, Section 711 "Modernization of the Visa Waiver Program" of the "Implementing Recommendations of the 9/11 Commission Act of 2007" ("9/11 Act") (110 PL 53) modifies the Visa Waiver Program under section 217 of the Immigration and Nationality Act (8 U.S.C. § 1187) to authorize this collection of information. The Secretary of Homeland Security is authorized to create the electronic travel authorization system and require aliens under the program to "electronically provide to the system biographical information and such other information as the Secretary of Homeland Security shall determine necessary." (8 U.S.C. § 1187(a)(11) as amended by 110 PL 53 sec. 711(d)). Collection of this information is mandatory for people from Visa Waiver Program countries who wish to travel to the United States.

personnel confirmed there are no instances in which social media information was the sole factor in an eligibility determination. Social media is considered to be one piece of a larger picture upon which eligibility decisions are made. Additionally, the information garnered from social media, whether the identifier was provided voluntarily by the applicant or found through the research of skilled CBP officers and analysts, is also used to determine the quality and integrity of other information provided by the applicant.

D. Data Minimization:

Requirement: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Review: To assess compliance with the data minimization requirements, PRIV reviewed PCR questionnaire responses; met with ESTA program and CBP PDO officials; and received a demonstration of the manual vetting process.

Finding: As outlined in the Rules of Behavior portion of the *Department's Privacy Policy for the Operational Use of Social Media*,[20] personnel should collect the minimum PII necessary for the proper performance of their authorized duties. PRIV was not able to adequately verify that CBP is adhering to this principle because, at this time there is not a mechanism in place for the ESTA program to collect, track, and analyze meaningful data that can be used to determine the efficacy of the collection of social media identifiers. Through the PCR process, CBP presented a small sample of success cases, in which the use of social media identifiers significantly aided in the screening and vetting of individuals seeking to travel to the United States under the VWP.

These success cases supported the use of social media information in order to assist in determining an individual's eligibility to travel to the United States under the VWP, to assist in determining if the applicant posed a law enforcement or security risk, as well as mitigate potentially derogatory information that would likely have resulted in the denial of an individual's ability to travel under the VWP.

While these cases highlight specific successful uses of social media identifiers in support of vetting and screening efforts, they are anecdotal and do not constitute a reliable, effective system for the tracking and analysis of qualitative data that could demonstrate the value of social media information to the VWP application process.

CBP was able to provide summary statistical information related to the number of applicants that provided some sort of response in the free-text fields for social media identifiers on the ESTA application. For example, in the first six months that social media identifiers were voluntarily collected as part of the ESTA application, 614,077 (approximately eight percent) of the

[20] *See:* DHS Instruction Number: 110-01-001 – Privacy Policy for Operational use of Social Media, *available at:* https://www.dhs.gov/sites/default/files/publications/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.

7,608,464 applicants provided a response. Additionally, the NTC presented figures associated with the social media platforms that identifiers were most commonly provided; with Facebook being the most frequent at nearly 73 percent, and Vine the least common at approximately eight percent.

However, at this time, CBP does not have an effective means of capturing data that identifies the operational impact that information collected from social media has on the successful adjudication of ESTA applications. In its current process, CBP notes if, and when, social media information was used as part of an application's adjudication in the form of general case notes, which CBP stated makes it difficult to query and retrieve data, and thereby unwieldy to track and analyze the use of social media identifiers.

> *Recommendation 2*: CBP should implement process or mechanism for tracking and measuring the viability and success of the collection and use of social media information as part of the screening and vetting process.

As evidence of the collaborative format that the PCR process adopts, PRIV identified this recommendation in the course of our review during in-person discussions with the ESTA staff and CBP PDO personnel. As of the date of this report, CBP is in the process of adding additional fields to capture more specific metrics specific to social media use for each reviewed ESTA case.

CBP stated that due to process constraints and technical limitations, it does not currently have an effective means of tracking the use of social media identifiers as a factor during the adjudication of ESTA applications. While PRIV understands additional effort will be required to implement a tracking mechanism that will facilitate data analysis, we think this capability should be developed to defend the collection of additional PII. Such data could assist in satisfying any internal requirements to assess the value of this information to the program, and would meet CBP's obligation as stated in the PIA to provide the Social Media Task Force with the results of this collection in order to evaluate its effectiveness in combatting national security threats.

The development of an automated solution for reports and analysis could not only reduce the currently cumbersome nature of producing data, but would also assist CBP in assessing the usefulness of this type of collection and strengthen the justifications[21] for the collection of such data in the context of the information collection reviews. The compilation and analysis of data associated with this effort could be used to justify and further demonstrate the utility of social media identifiers, as well as any information gleaned from social media platforms, to the screening and vetting process. Moreover, such analysis could lend insights in understanding how social media platforms are being used by those seeking to enter the United States with nefarious

[21] The Paperwork Reduction Act of 1995, as amended, 44 U.S.C. § 3501-3520, requires that the proposed information collection requests are necessary for proper performance of DHS functions, have practical utility, are not duplicative for the collection of information; and, to the extent practicable and appropriate, reduce the burden on persons providing information to DHS.

intents. Finally, the analysis could also permit DHS and CBP to determine whether more information is being collected than is necessary to fulfill its specified purposes.

The DHS Privacy Office recommends that CBP consider tracking the following information:

- the rates at which the provision of social media information directly supported the approval of an application or admission into the United States;
- the rates at which the provision of social media information directly supported denial of an ESTA application;
- the rates at which the provision of social media information directly supported an application's approval when initial derogatory information would have resulted in a denial;
- the frequency at which social media information was located and used when it was not provided voluntarily by the applicant;
- occurrences in which social media information was proven to be incorrect or found to be contrary to the information provided by an applicant; and
- information that could help to determine whether applicants who were denied an ESTA application based on national security grounds are providing social media identifiers, the degree at which they are being provided, and whether these identifiers are found to be valid.

E. Use Limitation:

Requirement: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Review: The DHS Privacy Office reviewed responses to the PCR questionnaire, the Privacy Notice, and the SORN in order to determine whether the use of information is compatible with the purposes for which it was collected.

Finding: Through the PCR process, PRIV found that CBP was operating in accordance with DHS policies, and within the boundaries of its legal authorities. Under 8 U.S.C. § 1187,[22] the Department is charged with reviewing the information of an alien seeking admission to the United States as a nonimmigrant visitor in order to make eligibility determinations. As outlined in the ESTA Privacy Impact Assessment (DHS/CBP/PIA-007(g)), information submitted via the ESTA application may be used and shared for national security and law enforcement vetting purposes, as well as VWP eligibility determinations. PRIV found that the information collected from ESTA applicants, including social media identifiers, was used and shared solely in support of screening and vetting efforts. Additionally, PRIV verified that all information shared in bulk outside of the Department was with other federal intelligence community partners, and in accordance with the provisions of the PIA and SORN.

[22] *See:* 8 U.S.C. § 1187, *available at:* https://www.gpo.gov/fdsys/pkg/USCODE-2011-title8/pdf/USCODE-2011-title8-chap12-subchapII-partII-sec1187.pdf.

With regard to social media identifiers that were provided by applicants or located through manual searches by CBP analysts, information was used to identify other potentially derogatory information and mitigate erroneous derogatory hits found during the automated review process.

F. Data Quality and Integrity:

Requirement: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

Review: The DHS Privacy Office reviewed the responses to the PCR questionnaire, CBP and NTC operational use of social media training materials, CBP's Operational Use of Social Media Rules of Behavior, and the ESTA Standard Operating Procedures. As part of this assessment, PRIV also reviewed the online ESTA application and met with ESTA Program staff to verify the means by which information is collected.

Finding: As required under the Privacy Act of 1974,[23] the Department must maintain accurate records. Failing to do so, as noted in *DHS Privacy Policy Guidance Memorandum 2017-01*,[24] could undermine efficient decision making and create the risk of errors. PRIV finds that CBP has implemented a number of functional and training processes designed to ensure that the data used by the ESTA program for the screening and vetting of applicants is accurate, relevant, timely, and complete.

Through the use of an online application that is generally completed by the individual seeking to travel to the United States under the VWP, CBP is involving the individual on which information is being collected, and can reasonably assume that it is accurate and complete. Furthermore, the application itself provides extensive instruction to the individual on the types of information that should be included within each field, helping to limit the likelihood that inaccurate data will be entered. However, the inclusion of free-text fields inherently creates the potential for individuals to enter information into fields incorrectly. CBP indicated that of the 614,077 applications in which an entry was made in the social media field of the ESTA application, not all of the submissions actually constituted a valid identifier. In some cases, applicants simply restated the platforms on which they maintain a social media presence, failing to provide information that would directly identify their account.

When an application is referred for manual review following automated checks, CBP has implemented a stringent examination process designed to facilitate the case-by-case adjudication of applications. Ultimately, highly trained CBP officers and analysts review the totality of information associated with an application in order to make a determination, and ensure that

[23] *See:* 5 U.S.C. § 552a, *available at*: https://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf.
[24] *See:* DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at 3 (April 27, 2017), *available at:* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

findings are based on information that is relevant and timely. All determinations are reviewed by a first line supervisor in order to verify that the findings are based on all available information and assessing the completeness and accuracy of the records. For those adjudications that result in adverse actions, NTC also employs a review by a second line supervisor. To further ensure that information used in the adjudication of ESTA applications is accurate, relevant, timely, and complete, NTC managers review case determinations; develop mentoring opportunities for officers and analysts; as well as review, update, and provide pertinent training.

To make certain that officers and analysts are using only information that has use and value during the screening and vetting process, the NTC employs a rigorous training regimen consisting of privacy-specific elements; CBP's Operational Use of Social Media instruction; specialized training focusing on the methods for searching social media and best practices developed by NTC; and on-the-job instruction in the use of tools, platforms, and methodologies in the identification of social media information that is relevant to the screening and vetting process. In an effort to further develop its capability and ensure the application of privacy protective practices, CBP is in the process of formalizing advanced social media and open source collection training curriculums.

> *Recommendation 3*: As a best practice, the ESTA Program should consider developing and providing more clear instructions to applicants aimed at reducing the inaccurate inclusion of non-identifier information in the social media 'free-text' portion of the online application.

G. Security:

Requirement: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Review: The DHS Privacy Office reviewed CBP's processes for providing system users with access to social media tools and information under the ESTA program, as well as the PCR questionnaire to gain an understanding of how data that is determined to be relevant to the screening and vetting process is maintained.

Finding: PRIV finds that CBP employs a number of effective safeguards in order to protect the information collected under the ESTA program from inappropriate access or use. Information collected via the ESTA program, including social media information, that results in adverse actions is maintained within the Automated Targeting System (ATS).[25] ATS complies with all aspects of the Federal Information Security Modernization Act of 2015 (FISMA),[26] and has a

[25] *See:* DHS/CBP/PIA-006 Automated Targeting System (January 13, 2017), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006e-ats-april2017.pdf.
[26] *See:* Public Law 113-283, 128 Stat. 3073 (December 18, 2014), *available at:* https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

current Authority to Operate (ATO).[27] An information system must be granted an ATO before it becomes operational, and must be re-authorized at least every three (3) years or if changes are made that affect the potential risk level of the system. ATS employs all applicable rules and policies, including all DHS automated systems security requirements in order to safeguard information. Access to information within the system is limited to those individuals who have an operational need to know, as well as a verified official duty and appropriate background level.

CBP also places strict limitations on the users' authorized to access social media information during the screening and vetting process. CBP limits the number of users that are authorized to engage in overt research and masked monitoring of social media.[28] These employees are provided with substantial training and operate under clearly defined policies regarding the use, handling, storage, and disclosure of information.[29] All personnel engaged in these efforts are also required to review and acknowledge an understanding of CBP's Social Media Rules of Behavior.[30]

H. Accountability and Auditing:

Requirement: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Review: The DHS Privacy Office reviewed responses to the PCR questionnaire, relevant CBP policies, and conducted discussions with CBP PDO and ESTA program personnel in order to gain an understanding of current accountability and access auditing processes.

Finding: PRIV finds that CBP employs a number of effective oversight methods to ensure that personnel with access to social media information in support of the ESTA program are operating in accordance with the DHS FIPPs and established policies. CBP PDO maintains oversight of users' privacy training completion, as well as the review and signed affirmation of Rules of Behavior, both of which must be completed annually, prior to the provision of access to social media information and tools. Additionally, the provision of access to social media information for operational purposes is only provided to individuals after the CBP PDO has reviewed and approved their request for access, as well as verified that an appropriate business justification and supervisory approval is in place, and all required documentation has been signed. For example, approved users are provided with masked monitoring access for a six-month period, at the end of which they are required to request access again. In order to extend their access for the

[27] *See:* Security Authorization Process Guide (March 16, 2015), *available at:* https://www.dhs.gov/sites/default/files/publications/Security%20Authorization%20Process%20Guide_v11_1.pdf.
[28] Masked monitoring allows certain CBP officers, agents, and analysts to use identities and credentials that do not identify a DHS or CBP affiliation, to log into social media. However, it does not include or allow engaging or interacting with individuals on or through social media. Overt research does not allow for the creation of accounts or logging onto social media sites, or otherwise interacting with individuals through social media.
[29] *See*: Customs and Border Protection Directive: 5410-003 – Operational Use of Social Media Directive (January 2, 2015), on file at DHS PRIV.
[30] *See:* CBP's Social Media Rules of Behavior, on file at DHS PRIV.

next six-month period, CBP PDO ensure that the individual provided training certificates and a signed Rules of Behavior document within the previous year. Access for users that fail to provide the necessary documentation will be suspended. Obtaining overt research access follows this same process, however the access period lasts one year. In essence, this incremental approach to user access facilitates the biannual/annual review of each users' access to ensure that proper training and documentation has been completed, and that a need for access still exists. CBP has reviewed its training program, and is currently in the process of formalizing advanced social media and open source collection curriculums.

The Rules of Behavior require that users understand that they will be held accountable for their actions while accessing and using government IT systems and social media sites. In order to verify that CBP personnel are adhering to the Rules of Behavior, CBP has established an audit capability for the social media profiles that are used in the screening and vetting of ESTA applications. In order to verify that CBP personnel were adhering to the stipulation in the Rules of Behavior that restricts officers and analysts from interacting with individuals through social media platforms, PRIV required that the NTC perform an audit of its social media accounts. This audit was ongoing at the completion of this PCR. In addition, NTC will work with PDO on future audits of the social media profiles used in screening and vetting of ESTA applications.

IV. Conclusion

The DHS Privacy Office commends U.S. Customs and Border Protection, including personnel from CBP PDO, the ESTA Program, and the NTC, for implementing robust safeguards to protect the personal information, specifically social media information, of ESTA applicants. CBP's operations in accordance with DHS's best practices and under the DHS FIPPs is representative of the manner in which privacy-sensitive programs should be operated. The recommendations of this PCR are intended to provide CBP with a means to further enhance the privacy-protective process already in place within the ESTA program.

This PCR provided the DHS Privacy Office with valuable insight into the privacy protective practices employed by CBP, the NTC, and the ESTA Program; and clearly demonstrates that the collection and use of social media information is in compliance with the requirements outlined in the ESTA PIA, DHS policies, and U.S. law. The DHS Privacy Office will continue to assess ESTA's level of compliance as needed, with the addition of any new functionality and information collections to the program. The requirement for future PCRs will be determined through discussions involving both operational staff, as well as oversight bodies at CBP and the DHS Privacy Office, and will be clearly outlined in future PIA updates. As such, the DHS Privacy Office requests that CBP PDO:

- monitor the implementation of the recommendations of this PCR;
- coordinate with ESTA Program and NTC personnel to brief the DHS Social Media Taskforce and/or Shared Services Vetting Board on the collection of social media identifiers, and the viability of their use in the screening and vetting process; and

- provide a written report on the implementation status of all recommendations within six months of this PCR's publication date. For any recommendations not implemented in that timeframe, or that CBP chooses not to implement, including any best practice recommendations, please explain why the recommendation was not implemented.

V. Privacy Compliance Review Approval

Responsible Official

Todd C. Owen
Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

John Wagner
Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

Approval Signature

[Original signed copy on file with the DHS Privacy Office.]

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security