Privacy Impact Assessment Update for

CBP Border Searches of Electronic Devices

DHS/CBP/PIA-008(a)

January 4, 2018

Contact Point
John Wagner
Deputy Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1610

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

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is publishing an updated Privacy Impact Assessment (PIA) to provide notice and a privacy risk assessment of the CBP policy and procedures for conducting searches of electronic devices pursuant to its border search authority. CBP is conducting this PIA update to describe recent changes to, and the reissuance of, CBP's policy directive governing border searches of electronic devices, CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018). CBP is conducting a privacy risk assessment of this updated policy as applied to any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players. Noting the evolution of the operating environment since the 2009 Directive was issued, along with advances in technology and other continuing developments, CBP reviewed and updated its Directive.

Overview

All merchandise and persons crossing the border, both inbound and outbound, are subject to inspection by CBP pursuant to its authority to enforce immigration, customs, and other federal laws at the border. CBP's search authority extends to all persons and merchandise, including electronic devices, crossing our nation's borders.[1] CBP conducts border searches of electronic devices in accordance with all legal requirements. CBP has imposed certain policy requirements, above and beyond prevailing legal requirements, to ensure that the border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust. In accordance with this newly updated and reissued policy,[2] CBP will continue to protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its border security and enforcement missions.[3]

As previously described in the original border searches of electronic devices PIA,[4] CBP identified two primary privacy risks regarding these types of searches. The first is whether CBP

[1] Pursuant to CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018), an electronic device is any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players.
[2] CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018). The 2009 Directive included a requirement to review the policy, as did the original Privacy Impact Assessment (*See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* www.dhs.gov/privacy).
[3] CBP's statutorily-prescribed duties include, among other things, ensuring the interdiction of persons and goods illegally entering or exiting the United States; enforcing the customs and trade laws of the United States; detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States; and safeguarding the border of the United States to protect against the entry of dangerous goods. 6 U.S.C. § 211.
[4] *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* www.dhs.gov/privacy.

has the appropriate authority to conduct this type of search at the border. The legal foundation for border searches of any object at the border, regardless of its type, capacity, or format, is well-established and is discussed in detail in the previously published 2009 PIA.[5] In general, border searches of electronic devices do not require a warrant or suspicion, but certain searches undertaken in the Ninth Circuit must meet a heightened standard.[6] The second privacy risk concerns CBP's potential over-collection of information from individuals due to the volume of information that is either stored on, or accessible by, today's electronic devices.

Individual privacy concerns are heightened due to the pervasiveness of smartphones and the volume and type of personal information they can store or that they can access through cloud-based applications. In the past, someone might bring a briefcase across the border that contains pictures of their friends or family, work materials, personal notes, diaries or journals, or any other type of personal information. Now due to the availability of electronic information storage locally on a device, as well as in cloud-based servers, the amount of personal and business information that may be hand-carried across the border, or accessible from a device carried across the border, by a single individual has increased exponentially. Further, today's smartphones and tablets are used for many reasons, including those that regularly involve communications and sharing views and personal thoughts. While someone may not feel that the inspection of a briefcase raises significant privacy concerns because of the more limited amount of information that could be searched, that same person may feel that a search of their electronic device is more invasive due to the amount of information potentially available on and now accessible by electronic devices.

Border Search Authority

CBP enforces and administers federal law at the border and facilitates the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department. Border searches of electronic devices are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. The border searches also help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. Searches can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, and export control violations. Searches can be vital to risk assessments that otherwise may be predicated on limited or no advance information about a given traveler or item, and they can enhance critical information sharing with, and feedback from, elements of the Federal Government responsible for analyzing terrorist threat information. Finally, searches at the border are often integral to a determination of an individual's intentions upon entry to the United States and provide additional information relevant to admissibility under immigration laws.

[5] *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* www.dhs.gov/privacy.
[6] *See Cotterman v. United States*, 709 F.3d 952 (9th Cir. 2013).

CBP's border authorities permit the inspection, examination, and search of vehicles, persons, baggage, and merchandise to ensure compliance with any law or regulation enforced or administered by CBP. All travelers entering the United States are required to undergo customs and immigration inspection to ensure they are legally eligible to enter and that their belongings are not being introduced contrary to law. CBP's authorities to conduct searches of travelers and their merchandise entering or leaving the United States will be referred to in this PIA as "border search authority." CBP may search electronic devices, as with any other belongings, pursuant to border search authority.

CBP's border search authority applies at the physical border, the functional equivalent of the border (for example, international airports in the interior), or the extended border, as those terms are defined under applicable law. The border search authority applies to both inbound and outbound travelers and merchandise, including electronic devices.

If Selected for a Search of Your Electronic Device

CBP searches only a fraction of international travelers' electronic devices.[7] Travelers arriving at a port of entry must present themselves and their effects for inspection. During the border inspection, a CBP Officer checks the traveler's documentation and reviews relevant information (including relevant law enforcement information and "lookouts"[8]). The Officer may verbally request additional information from the traveler and may perform a basic search (defined further below) of the traveler's electronic device with or without suspicion. If the CBP Officer determines that the traveler warrants further examination, he or she will refer the traveler for additional scrutiny, known as "secondary inspection," which may include a basic or advanced search of the traveler's electronic devices. CBP documents relevant information regarding border inspections, including inspections of both basic and advanced searches, in its primary law enforcement system, TECS.[9]

CBP Officers document searches of electronic devices in the "Electronic Media Report" module of TECS, which provides information on why the traveler was selected for an examination. Furthermore, at every stage after the traveler is referred to "secondary inspection," CBP maintains records of the examination, detention, retention, or seizure of a traveler's property, including any electronic devices. Additionally, signage is posted throughout the port areas informing travelers

[7] In FY17, CBP conducted 30,200 border searches, both inbound and outbound, of electronic devices. CBP searched the electronic devices of more than 29,200 arriving international travelers, affecting 0.007 percent of the approximately 397 million travelers arriving to the United States. Of the more than 390 million arriving international travelers that CBP processed in FY16, 0.005 percent of such travelers (more than 18,400) had their electronic devices searched.

[8] As part of processing individuals at the border, DHS/CBP conducts pre-arrival or pre-departure TECS queries, which include checks against lookouts, such as "wants and warrants," watchlist matches, etc.

[9] For a complete overview of TECS, its functions, and the associated privacy risks, *see* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (December 22, 2010) and DHS/CBP/PIA-021 TECS System: Platform (August 2016), *available at* www.dhs.gov/privacy.

that all vehicles, other conveyances, persons, baggage, packages, or other containers are subject to detention and search. Specifically regarding border searches of electronic devices, CBP has created a tear-sheet[10] to provide travelers who have questions or concerns regarding the search of their electronic device.

Reason for the PIA Update

CBP previously published a PIA[11] examining the privacy impact of the procedures for searching electronic devices at the border in 2009. In the ensuing years, there have been a number of significant developments, including:

- evolution in the operational threat environment;
- the proliferation of various forms of electronic devices, specifically tablets and smartphones, and the advancement of technology that has resulted in increased capacity to store and transport information, including sensitive and personal information;
- the rise of cloud-based applications accessible by electronic devices, that permit storage of even greater amounts of information than could be stored on an individual device;
- continuing public attention to issues of privacy and government collection of personal information; and
- CBP's issuance of an updated policy for *Border Searches of Electronic Devices* (January 2018).

The 2009 PIA provides a comprehensive discussion of CBP's searches of electronic devices under border search authority. This PIA update provides both an update to that analysis, with additional detail regarding how CBP uses information collected from electronic devices. CBP is conducting this PIA to provide notice and a privacy risk assessment of (1) policy changes due to the update and reissuance of the CBP *Border Search of Electronic Devices* Policy and (2) changes in where and how CBP stores information extracted from electronic devices.

1. Update and Reissuance of the CBP Border Search of Electronic Devices Policy

In tandem with this PIA, CBP publicly released an updated *Border Searches of Electronic Devices* policy. The purpose of this CBP-wide policy remains the same: to provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, tablets, removable media, disks, drives, tapes, mobile phones, cameras, music and other media players, and any other communication, electronic, or digital devices subject to inbound and outbound border searches by CBP. However, there are several changes from the original 2009 policy.

[10] *See* https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf.
[11] *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* www.dhs.gov/privacy.

A. Types of CBP Border Searches of Electronic Devices

The Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority – conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of the Directive, this excludes actions taken to determine if a device functions (*e.g.*, turning an electronic device on and off); actions taken to determine if physical contraband is concealed within the device itself; or the review of information voluntarily provided by an individual in an electronic format (for example, when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). The Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, abandonment, or in response to exigent circumstances; it does not limit CBP's ability to record impressions relating to border encounters; nor does it restrict the dissemination of information as required by applicable statutes and Executive Order.

CBP Officers are trained to assess a "totality of circumstances" when making determinations on the appropriate actions to take during a border inspection. CBP may engage in various actions during a border inspection, such as an examination of the traveler belongings including their electronic devices. In the context of border searches of electronic devices, a search may be conducted for a variety of reasons. For example, if the traveler is suspected of possessing child pornography or trafficking a controlled substance, that traveler may be referred for additional scrutiny and a search of their device. A search of an electronic device may also assist a CBP Officer in verifying information that may be pertinent to the admissibility of a foreign national who is applying for admission.

With respect to border searches of information contained in electronic devices, the original 2009 policy did not differentiate between the types of searches that CBP conducts on an electronic device. Under the new 2018 policy, CBP has updated the definitions of these searches and outlined the procedures that apply to each respective type of search. CBP now follows different procedures depending on whether the search is a "basic search" or an "advanced search." As explained in greater detail below, a basic search may be conducted with or without suspicion, while the Directive requires, strictly as a matter of policy, additional justification for an advanced search.

Notably, while a basic search is not a necessary precursor to an advanced search, information identified during a basic search may lead to an advanced search, consistent with Section 5.1.4 of the Directive.

Basic Search

A basic search is defined in CBP policy as "any border search of an electronic device that is not an advanced search [as described below]. In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information

encountered at the border, subject to the requirements and limitations provided herein and applicable law."[12]

A CBP Officer may perform a basic search of the electronic device in front of the passenger with or without suspicion. This search may reveal information that is resident upon the device and would ordinarily be visible by scrolling through the phone manually (including contact lists, call logs, calendar entries, text messages, pictures, videos, and audio files). Unlike an advanced search (described below), the basic search does not entail the connection of external equipment to review, copy, and/or analyze its contents. Following the examination of the device, the CBP Officer conducting the inspection enters a record of the interaction, including a record of any electronic devices searched, into the TECS module.

Pursuant to law, CBP undertakes basic searches with or without suspicion. Following a basic search, if CBP is satisfied that no further examination is needed, the electronic device is returned to the traveler and he or she is free to proceed. In this situation, no receipt to document chain of custody is given to the traveler because the device has not been detained or seized. Upon traveler request and when operationally feasible, CBP Officers may conduct the basic examination of an individual's electronic device in a private area away from other travelers.

Advanced Search

An advanced search is defined in CBP policy as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.[13]

If an Officer determines that there is reasonable suspicion of activity in violation of laws enforced or administered by CBP, or that there is a national security concern, the CBP Officer may conduct an advanced search with supervisory approval. An advanced examination of an electronic device may involve the copying of the contents of the electronic device for analysis at a later time.

CBP thoroughly documents all border searches of electronic devices. For both basic and advanced searches, CBP Officers are trained to provide all pertinent information related to the search of the electronic device, including the name of the Officer performing the search, the date the search was performed, the name of the owner of the electronic device, a physical description

[12] CBP Directive No. 3340-049A at 5.1.3.
[13] CBP Directive No. 3340-049A at 5.1.4.

of the device, and factors related to initiating the search. At times it is necessary to detain a device for continuation of the border search for a period after an individual's departure from the port or other location of detention. When CBP detains devices pursuant to the updated directive, the traveler is issued a Customs Form (CF) 6051D.[14]

Prior to copying the contents of an electronic device, the inspecting CBP Officer must obtain supervisory approval. Furthermore, data copied from the phone is limited to what is on the physical device. CBP border searches extend to the information that is physically resident on the device and do not extend to information that is located solely on remote servers.

B. Policy-based Limits and Controls on Border Searches of Electronic Information

i. *Reasonable Suspicion or National Security Concern*

As described above, an advanced search is defined in CBP policy as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." The Directive requires that in instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.[15]

This is a significant shift from the original 2009 policy. CBP now defines advanced searches, and as a matter of nationwide policy, provides that they will be conducted where there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or when there is a national security concern. CBP now affirmatively imposes policy requirements on advanced searches, above and beyond constitutional and legal requirements, to ensure that the border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

By applying a heightened standard to all advanced searches of electronic devices, CBP is self-imposing greater policy controls over its border search authority. This shows that CBP is taking responsible steps to ensure and maintain individual privacy and public trust, while still meeting its enforcement mandates.

---

[14] Customs Form (CF) 6051D is provided to the traveler as a receipt. This form contains contact information for the traveler and the CBP Officer to ensure each party can contact the other with questions or for retrieval of the electronic device at the conclusion of the border search. From the time the electronic device is detained to the time it is returned to the traveler, the device is kept in secured facilities with restricted access at all times.

[15] CBP Directive No. 3340-049A at 5.1.4.

ii. Restriction on CBP Access to Information in the "Cloud"

In the 2018 Directive, CBP has formally clarified the scope of the information it accesses when conducting border searches of electronic devices. The updated policy clarifies that a border search includes an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications.[16] For both basic and advanced searches, Officers may not intentionally use the device to access information that is solely stored remotely.[17] Prior to beginning a basic or advanced search, CBP Officers must take steps to ensure that a device is not connected to any network. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (*e.g.*, by placing the device in airplane mode), or, where warranted by national security, law enforcement, Officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.[18]

iii. Treatment of Privileged Information

CBP border searches of electronic devices have raised concerns regarding potential access to, and handling of, attorney-client privileged information. While the original CBP policy provided that privileged information must be protected in accordance with applicable law, and required that Officers coordinate with the CBP Office of Chief Counsel (OCC), the updated directive provides additional detail regarding the procedures CBP Officers follow when they encounter information that they identify as privileged or over which a privilege has been asserted. The 2018 Directive maintains the provisions from the 2009 Directive regarding the treatment of other possibly sensitive information, such as medical records and work-related information carried by journalists, which shall still be handled in accordance with any applicable federal law and CBP policy. CBP Officers' questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel office, and this consultation shall be noted in appropriate CBP systems, as required previously.

If an Officer encounters information identified as, or that is asserted to be, attorney-client privilege information or attorney work product, the Officer must seek clarification from the individual asserting the privilege as to the specific files, attorney or client names, or other particulars that may assist CBP in identifying privileged information. Pursuant to the updated policy, CBP Officers shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, or categories of files, attorney or client names, email addresses, or phone numbers, or other particulars that may assist CBP in identifying

[16] CBP Directive No. 3340-049A at 5.1.2.
[17] CBP Directive No. 3340-049A at 5.1.2.
[18] CBP Directive No. 3340-049A at 5.1.2.

privileged information.[19] Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the Associate/Assistant Chief Counsel office.[20] In coordination with the Associate/Assistant Chief Counsel office, which will coordinate with the U.S. Attorney's Office as needed, Officers will ensure the segregation of any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also ensuring that CBP accomplishes its critical border security mission. This segregation process will occur through the establishment and employment of a Filter Team comprised of legal and operational representatives, or through another appropriate measure with written concurrence of the Associate/Assistant Chief Counsel office.

At the completion of the CBP Filter Team review, unless any materials are identified that indicate an imminent threat to homeland security, copies of materials maintained by CBP and determined to be privileged will be destroyed, except for any copy maintained in coordination with the Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.[21]

iv. Handling of Passcode-Protected or Encrypted Information

The 2009 policy was silent regarding CBP's handling of passcode-protected or encrypted information. As technology has enabled more sophisticated data security safeguards to be employed over electronic devices, CBP has self-imposed controls over how and when it will access, store, and destroy information that is passcode-protected or encrypted.

Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents.[22] Officers may request passcodes or other means of access to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained.

Any passcodes or other means of access provided by the traveler will be used as needed to facilitate the examination; however, they must be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be used to access information that is only stored remotely.[23] The CBP Privacy Officer shall conduct a CBP Privacy Evaluation of this requirement

[19] CBP Directive No. 3340-049A at 5.2.1.1.
[20] CBP Directive No. 3340-049A at 5.2.1.2.
[21] CBP Directive No. 3340-049A at 5.2.1.3.
[22] CBP Directive No. 3340-049A at 5.3.1.
[23] CBP Directive No. 3340-049A at 5.3.2.

within one year of publication of this PIA. The Privacy Evaluation will be shared with the DHS Privacy Office.

If an Officer is unable to complete an inspection of an electronic device because it is protected by a passcode or encryption, the Officer may detain the device pending a determination as to its admissibility, exclusion, or other disposition.

2. Storage of Information Extracted from an Electronic Device in the Automated Targeting System

The 2009 Directive provided for the retention of information relating to immigration, customs, and other enforcement matters, if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. Since that time, CBP published a Privacy Impact Assessment Update regarding CBP's use of the Automated Targeting System (ATS)[24] to store information copied and stored from a traveler's electronic device. To further CBP's border security mission, CBP may use ATS to further review, analyze, and assess the information physically resident on the electronic devices, or copies thereof, that CBP collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain information from the physical device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in the ATS-Targeting Framework (TF) for purposes of CBP's border security mission, including identifying individuals who and cargo that need additional scrutiny. CBP may use ATS-TF to vet the information collected from the electronic devices of individuals of concern against CBP holdings and create a report which includes data that may be linked to illicit activity or actors. Information from electronic devices uploaded into ATS will be normalized[25] and flagged as originating from an electronic device.

Section 5.5.1.2 of the 2018 CBP directive, *Border Searches of Electronic Devices*, provides for retention of information in CBP Privacy Act-Compliant Systems and states that without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and/or other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained.

ATS may be used to conduct an analytic review of the information and will transfer results of that review to ATS-TF. ATS-TF may retain the analytic review, which includes the information that may be linked to illicit activity or illicit actors and the underlying information relating to immigration, customs, and/or other enforcement matters for the purposes of ensuring compliance with laws CBP is authorized to enforce and to further CBP's border security mission,

[24] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[25] Normalization is the process of organizing data in a database to reduce redundancy and ensure that related items are stored together.

including identifying individuals and cargo that need additional scrutiny and other law enforcement, national security, and counterterrorism purposes. For example, CBP may use ATS to link a common phone number to three separate known or suspected narcotics smugglers, which may lead CBP to conduct additional research and, based on all available information, further illuminate a narcotics smuggling operation.[26]

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(2), states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 (Section 208) and the Homeland Security Act of 2002 (Section 222). Given that the search, detention, seizure, and retention of electronic devices through a border search is a DHS practice, CBP is conducting this PIA as it relates to the DHS construct of the FIPPs.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

Due to the ongoing public interest of CBP's use of its border search authority, CBP has endeavored to provide as much notice and transparency regarding its border searches of electronic devices as possible. As described in the original PIA, CBP provides signage in all inspection areas that all vehicles, other conveyances, persons, baggage, packages, or other containers are subject to

[26] For a full description of the ATS process for storing information extracted from electronic devices, *please see* Addendum 2.3 of the DHS/CBP/PIA-006(e) Automated Targeting System PIA, "Retention of Information from Electronic Devices in the Automated Targeting System-Targeting Framework" (April 28, 2017), *available at* www.dhs.gov/privacy.

detention and search. CBP has created a tear-sheet[27] to provide travelers who have questions or concerns regarding the search of their electronic device. CBP has also published its previous, and newly updated, policies regarding border searches of electronic devices, and is publishing this PIA in tandem. CBP has also posted information on its website regarding the issue of border searches of electronic devices.[28]

In addition, at the time of the search, as a matter of policy, CBP will notify the individual subject to search of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. If the Officer or other appropriate CBP official determines that the fact of conducting this search cannot be disclosed to the individual transporting the device without impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld.[29]

As in 2009, CBP may retain information obtained from searches of electronic devices in a Privacy Act compliance system of records, consistent with the purpose of the collection. CBP has provided additional notice to the public by publishing system of records notices regarding these collections. Some of the SORNs that may be applicable to information obtained from a border search of electronic devices are:

- DHS/CBP-006 Automated Targeting System[30] covers information that is extracted from an advanced search of a device and stored in the ATS-Targeting Framework.
- DHS/CBP-011 U.S. Customs and Border Protection TECS[31] covers among other things, any records of any inspections conducted at the border by CBP, including inspections of electronic devices, including factors on the initiation of the search as described in the TECS Electronic Media Report module.
- DHS/CBP-013 Seized Assets and Case Tracking System (SEACATS)[32] provides notice regarding any seizures, fines, penalties, or forfeitures associated with the seizure of electronic devices.

These SORNs provide overall notice and descriptions of how CBP functions in these circumstances, the categories of individuals, the types of records maintained, the purposes of the examinations, detentions, and seizures, and the reasons for sharing such information. Any third party information that is retained from an electronic device and maintained in a CBP system of records will be secured and protected in the same manner as all other information in that system.

---

[27] *See* https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf.
[28] *See* CBP Search Authority, *available at* https://www.cbp.gov/travel/cbp-search-authority.
[29] CBP Directive at 5.4.1.3.
[30] DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297.
[31] DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.
[32] DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.

Privacy Risk: There is a risk that individuals do not have notice that CBP may search their electronic devices as part of a border search.

Mitigation: This risk is mitigated. CBP has been proactive in its notice and transparency about this program, to include publicly releasing the policy for these searches and publishing corresponding PIAs. In addition, at the time of collection, travelers are provided signage in the inspection area and specialized tear sheets regarding border searches of electronic devices.

Searches of electronic devices should be conducted in the presence of the individual whose information is being examined unless there are national security, law enforcement, officer safety, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search itself. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

In very few cases, CBP is unable to provide notice to travelers that their electronic devices are being searched due to national security or serious law enforcement concerns, when providing notice at the time of collection may compromise ongoing investigations or increase a national security threat. Due to the limited nature of this circumstance, and the public signage and information available regarding this program, this risk remains mitigated.

2. Principle of Individual Participation

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

There have been no changes to individual participation since the 2009 PIA. As described then, a traditional approach to individual participation is not always practical for CBP due to its law enforcement and national security missions. Allowing the traveler to dictate the extent of a border search and the detention, seizure, retention, and sharing of the information encountered during that search would interfere with the U.S. government's ability to protect its borders and diminish the effectiveness of such searches, thereby lessening our overall national security.

Privacy Risk: There is a risk that individuals cannot consent to, or opt-out of, a border search.

Mitigation: This risk is partially mitigated. All belongings a traveler carries when crossing the U.S. border, including electronic devices,[33] are subject to search by CBP pursuant to its

[33] Pursuant to CBP Directive No. 3340-049A "Border Searches of Electronic Devices" (January 2018), an electronic device is any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players.

authority to enforce immigration, customs, and other federal laws at the border. Border searches can implicate ongoing law enforcement investigations, or involve law enforcement techniques and processes that are highly sensitive. For these reasons, it may not be appropriate to allow the individual to be aware of or participate in a border search. Providing individuals of interest access to information about them in the context of a pending law enforcement investigation may alert them to or otherwise compromise the investigation.

To help partially mitigate this risk, CBP will involve the individual in the process to the extent practical given the facts and circumstances of the particular border search. In particular, pursuant to the newly issued policy, CBP may ask individuals to provide passcodes or other means to access the device, or clarify what specific information on their device is privileged, thereby involving the traveler in the search.[34] Should the border search continue after an individual's departure from the port or other location of detention, the traveler will be notified if his or her electronic device is detained or seized. In instances when direct individual participation is inappropriate, substantial transparency, well-documented processes, well-trained CBP Officers, safeguards, and oversight will help to ensure the accuracy and integrity of these processes and information.

3. Principle of Purpose Specification

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

The authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[35] "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border."[36] "Routine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant." [37] Additionally, the authority to conduct border searches extends not only to persons and merchandise entering the United States, but applies equally to those departing the country.[38]

---

[34] CBP Directive No. 3340-049A at 5.2.1.1 (regarding privilege) and at 5.3.1 (regarding passcodes and encryption).
[35] *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004).
[36] *Id*. at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).
[37] *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).
[38] *See, e.g., United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995); *United States v.*

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel.[39] Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign.[40]

In addition to longstanding federal court precedent recognizing the constitutional authority of the U.S. Government to conduct border searches, numerous federal statutes and regulations also authorize CBP to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property, such as electronic devices.[41] These authorities support CBP's enforcement and administration of federal law at the border and facilitate the inspection of merchandise and people to fulfill the immigration, customs, agriculture, and counterterrorism missions of the Department.[42]

Because CBP enforces federal law at the border, information may be detained or retained from a traveler's electronic device for a wide variety of purposes. CBP may use data contained on electronic devices to make admissibility determinations or to identify evidence of violations of law, including importing obscene material, drug smuggling, other customs violations, or terrorism, among others. The information may be shared with other agencies that are charged with the enforcement of a law or rule if the information is evidence of a violation of such law or rule. In appropriate circumstances, CBP may also convey electronic device or information obtained from the device with third parties for the purpose of obtaining technical assistance to render a device or its contents in a condition that allows for inspection. Consistent with applicable laws and SORNs, information lawfully obtained by CBP may be shared with other state, local, federal, and foreign law enforcement agencies in furtherance of enforcement of their laws.

Privacy Risk: There is no privacy risk to purpose specification. The legal precedent is clear, and all information is maintained, stored, and disseminated consistent with published systems of records notices.

Ezeiruaku, 936 F.2d 136, 143 (3d Cir. 1991) *United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983).

[39] *See Flores-Montano*, 541 U.S. at 154 (noting that "the expectation of privacy is less at the border than it is in the interior").

[40] *See Boumelhem*, 339 F.3d at 423.

[41] *See, e.g.*, 8 U.S.C. §§ 1225; 1357; 19 U.S.C. §§ 482; 507; 1461; 1496; 1581; 1582; 1589a; 1595a; *see also* 19 C.F.R. § 162.6 ("All persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer.").

[42] This includes, among other things, the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting the United States"; "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband;" and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons." 6 U.S.C. § 211.

4. Principle of Data Minimization

Principle: *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). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

Over-collection of, or access to, information by CBP Officers as part of their border search of electronic devices is a primary privacy concern for the traveling public. As stated above, with the rise in storage available on small electronic devices, the amount of information that can be accessed by a device using cloud-based applications, and the amount of personal information that individuals now store on their electronic devices, travelers may be wary of letting a CBP Officer scroll through such a device. Because of the volume of information available on, or accessible by, electronic devices, CBP has imposed policy based limitations on CBP's retention of information. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer. However, without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice.

Privacy Risk: There is a risk that CBP may access traveler information that is stored in the cloud, such as information from social network sites, web-based email services, online banking, and other highly sensitive information.

Mitigation: This risk is mitigated. Border searches of electronic devices include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (*e.g.*, by placing the device in airplane mode), or, when warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

Privacy Risk: There is a risk that CBP will retain information obtained from an electronic device for a period longer than necessary to make an admissibility determination or take a law enforcement action.

Mitigation: This risk is mitigated. A CBP Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days. Devices must be presented in a manner that allows CBP to inspect their contents. Any device not presented in such a manner may be subject to exclusion, detention, seizure, or other appropriate action or disposition.

If a device is detained, supervisory approval is required for detaining electronic devices, or copies of information contained therein, for continuation of a border search after an individual's departure from the port or other location of detention. Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager approval is required to extend any such detention beyond five (5) days. Extensions of detentions exceeding fifteen (15) days must be approved by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or, other equivalent manager, and may be approved and re-approved in increments of no more than seven (7) days. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems.

If after reviewing the information pursuant to the time frames above, there is no probable cause to seize the device or the information contained therein, any copies of the information held by CBP must be destroyed, and any electronic device must be returned, unless CBP retains information relating to immigration, customs, or other enforcement matters where such retention is consistent with the applicable system of records notice. Upon this determination, the copy of the information will be destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system and which must be no later than twenty-one (21) days after such determination.

CBP has self-imposed these data retention requirements as a matter of policy pursuant to the CBP *Border Searches of Electronic Devices* policy to help mitigate this risk. To provide an additional layer of oversight and transparency, the CBP Privacy Officer will conduct a CBP Privacy Evaluation of these records within one year of the publication of this PIA and share the results of the Privacy Evaluation with the DHS Privacy Office.

5. Principle of Use Limitation

Principle: *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.*

As with data minimization, the same privacy concerns arise for use limitation. The more information that Officers have available to them, the greater the risk that they may use the

information in a manner that is inconsistent with the purpose and authority for collection. Also, CBP is not always technically able to conduct a search of a device without requesting assistance. In this situation, there are privacy risks regarding the use of information by the assisting entity.

As a federal law enforcement agency, CBP has broad authority to share lawfully seized and/or retained information with other federal, state, local, and foreign law enforcement agencies in furtherance of law enforcement investigations, counterterrorism, and prosecutions (consistent with applicable SORNs). To ensure that a traveler's seized and/or retained information is used for the proper purpose, all CBP employees with access to the information are trained regarding the use, dissemination, and retention of PII. Employees are trained not to access the traveler's information without an official need to know and to examine only that information that might pertain to their inspection or investigation; access to such information is tracked and subject to audit. Any such sharing is pursuant to a published routine use and documented in appropriate CBP systems and/or is recorded by those systems' audit functions.

Privacy Risk: There is a risk that in the course of seeking technical assistance from an external agency to conduct an analysis of a device, the external agency will retain the information exploited from the device inconsistent with CBP policy.

Mitigation: This risk is partially mitigated. All electronic devices, or copies of information contained therein, provided to an assisting entity may be retained for the period of time needed to provide the requested assistance to CBP, unless the assisting entity has its own independent authority to maintain the information. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible. The assisting entity should destroy all copies of the information conveyed unless it invokes its own independent authority to retain the information.

If an assisting entity elects to continue to retain or seize an electronic device or information contained therein, that agency assumes responsibility for processing the retention or seizure. Copies may be retained by an assisting entity only if and to the extent that it has the independent legal authority to do so – for example, when the information relates to terrorism or national security and the assisting entity is authorized by law to receive and analyze such information. In such cases, the retaining entity should advise CBP of its decision to retain information under its own authority.

Privacy Risk: Because many individuals use the same passcodes or PINs across multiple devices or services, there is a risk that CBP may use a previously collected passcode, PIN, or other means of access to access a recently searched electronic device.

Mitigation: This risk is mitigated. As described above, as technology has enabled more sophisticated data security safeguards to be employed over electronic devices, CBP has self-imposed controls over how and when it will access, store, and destroy information that is passcode-protected or encrypted.

Travelers are obligated to present electronic devices and the information contained therein in a condition that allows inspection of the device and its contents. If presented with an electronic device containing information that is protected by a passcode or encryption or other security mechanism, an Officer may request the individual's assistance in presenting the electronic device and the information contained therein in a condition that allows inspection of the device and its contents.[43] Officers may request passcodes or other means of access to facilitate the examination of an electronic device or information contained on an electronic device, including information on the device that is accessible through software applications present on the device that is being inspected or has been detained, seized, or retained.

Any passcodes or other means of access provided by the traveler will be retained as needed to facilitate the examination, however they must be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be used to access information that is only stored remotely.[44] The CBP Privacy Officer shall conduct a CBP Privacy Evaluation of this requirement within one year of publication of this PIA and share the results of the Privacy Evaluation with the DHS Privacy Office.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

There are no changes to the privacy risks surrounding data quality and integrity since the original PIA was published. As described in 2009, inaccurate, irrelevant, untimely, or incomplete information may result in cases moving to prosecution when none is warranted, or may result in cases being dismissed when a violation has occurred. To ensure the PII is accurately recorded, CBP takes precautions to prevent the alteration of the information on the electronic device. To ensure the PII is relevant and timely, CBP detains the information from the traveler's electronic device at the time the traveler attempts to enter the United States. Further, CBP keeps the information from a traveler's electronic device only until the border search has reached a conclusion, at which time copies of the information are destroyed, unless further retention is appropriate under applicable law and policy and consistent with the appropriate retention schedule. Information entered into TECS, SEACATS,[45] and other systems of records are kept with annotations noting the time they were added to the file for contextual relevancy.

[43] CBP Directive No. 3340-049A at 5.3.1.
[44] CBP Directive No. 3340-049A at 5.3.2.
[45] DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.

7. Principle of Security

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

There are no changes to the privacy risks surrounding security since the original PIA was published. CBP will appropriately safeguard information retained, copied, or seized from an electronic devices and during conveyance. [46] Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during conveyance such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager and the CBP Office of Professional Responsibility.

In addition, CBP employees must pass a full background investigation and be trained regarding the access, use, maintenance, and dissemination of PII before being given access to the system maintaining the information. Training materials are routinely updated, and the employees must pass recurring TECS certification tests in order to maintain access. While these procedures generally prevent employees from accessing information without some assurance of security, specific security measures are in place to prevent unauthorized access, use, or dissemination for each set of information. Employees must have an official need to know in order to access the information. This need to know is checked by requiring supervisory approval before information is scanned or copied from a traveler's electronic device, and before information is shared outside of CBP.

8. Principle of Accountability and Auditing

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

As a matter of policy, CBP has created robust auditing and accountability measures for this program, in part due to the heightened privacy concerns regarding border searches of electronic devices. All Officers performing a border search are responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Customs Form (CF) 6051D[47] when appropriate, and creation and/or

[46] CBP Directive No. 3340 at 5.5.1.5.
[47] Customs Form (CF) 6051D is provided to the traveler as a receipt. This form contains contact information for the traveler and the CBP Officer to ensure each party can contact the other with questions or for retrieval of the electronic device at the conclusion of the border search. . From the time the electronic device is detained to the time it is returned to the traveler, the device is kept in secured facilities with restricted access at all times.

updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate. In addition, the DHS Office of the Inspector General is required by statute to conduct annual reviews, over the course of three consecutive years, as to whether CBP's border searches of electronic devices are being conducted in accordance with statutorily-required standard operations procedures for such searches.[48]

Privacy Risk: There is a risk of lack of oversight and accountability of this program.

Mitigation: This risk is partially mitigated. The robust supervisory reviews and controls described in the original PIA still remain. To continue to provide metrics and accountability regarding this program, CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers.

The updated policy directive also directs that the CBP Management Inspection[49] will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive. In addition, the CBP Privacy Officer shall conduct a CBP Privacy Evaluation of the privacy controls noted above in the PIA.

Responsible Official

Debra L. Danisek
Privacy Officer
Office of the Commissioner, Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

[48] 6 U.S.C. § 211(k)(5).
[49] The CBP Management Inspections Division is a division of the Office of Professional Responsibility that provides internal audit and oversight for CBP operations.