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.

Privacy Impact Assessment
for the

Border Surveillance Systems (BSS)

DHS/CBP/PIA-022

August 29, 2014

Contact Point
Douglas Harrison
Associate Chief, Office of Border Patrol
U.S. Customs and Border Protection (CBP)
(202) 344-2050

Reviewing Official
Karen Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Border Surveillance Systems (BSS) are a combination of surveillance systems deployed to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. The BSS include commercially available technologies such as fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors. CBP is conducting this PIA because the BSS collect and process Personally Identifiable Information (PII) including video images, photographs, radio frequency emissions, and location information. In addition, the Secure Border Initiative-net (SBInet) Program PIA, which addresses the SBInet Southern Border and Northern Border Projects will be retired upon publication of this PIA.

Overview

CBP is responsible for securing the borders of the United States while facilitating lawful international trade and travel. CBP employs various technologies to enforce hundreds of U.S. laws and regulations at the border, including immigration and narcotics enforcement laws. BSS are a combination of surveillance technologies designed to assist CBP in detecting, identifying, apprehending, and removing persons illegally entering the United States at and between ports of entry and enforcing U.S. law. BSS may also monitor a particular individual or location as part of a law enforcement investigation, and as evidence if the apprehension of the individual results in criminal proceedings. BSS that are located across urban, rural, and remote areas along the U.S. border include tethered aerial video, radars, mobile and fixed ground video with day and night thermal capabilities, ground sensors, radio frequency sensors, ultra-light aircraft detection, and acoustic sensing devices. Each surveillance system is deployed taking into account the surrounding terrain and population. DHS is conducting this PIA because BSS collect and process PII, including video, images, radio frequency emissions, and location information.

DHS created the SBInet Program in November 2005, to reduce illegal immigration and secure the nation's borders by providing CBP more comprehensive situational awareness along the U.S. border.[1] The "Project 28" (P-28) initiative was a concept demonstration prototype for the SBInet Program followed by a geographical expansion and an operational capabilities enhancement known as the SBInet Southern Border and SBInet Northern Border Projects. On January 14, 2011, DHS Secretary Janet Napolitano directed CBP to end the SBInet Program as originally conceived after assessing the efficiency of the SBInet Program.

CBP replaced the SBInet Program with BSS, a new border security technology plan using

[1] SBInet (CBP's initial border surveillance technology initiative) began as an implementation of the Executive Branch Program, "Border Security and Control Between the Ports of Entry," as authorized under the Secure Fence Act of 2006, Pub. L. #109-367, 8 U.S.C. § 1701 Note; Title 8, C.F.R, Section 287. Initially piloted as Project 28, the program sought to integrate the use of fixed tower cameras, ground sensors, and a Common Operational Picture to enhance border security and combat illegal immigration.

existing and proven technology tailored to distinct terrain and population density. BSS represent a reassessment of the need to provide increased situational awareness for CBP in areas that present capability gaps based on the lessons learned from the P-28 and SBInet Projects. BSS include the Block 1 (part of SBINet) and the Northern Border Remote Video Surveillance as well as the following new projects: Integrated Fixed Tower (IFT), Remote Video Surveillance System (RVSS), Intelligent Computer Assisted Detection (ICAD), Law Enforcement Technical Collection (LETC), Mobile Video Surveillance Systems (MVSS), Mobile Surveillance Capability (MSC), Agent Portable Surveillance System (APSS), Ultra-Light Aircraft Detection (ULAD), and Tethered Aerostat Radar System (TARS). BSS may capture PII in urban, rural, and remote areas along the U.S. border through video cameras, laser range finders, radar, radio frequency sensors and acoustic devices, or some combination thereof. Not all data collected by BSS may be used to identify an individual at the time of collection; however, data captured using the various BSS may later be associated with an individual. Below is a description of the different types of systems BSS uses:

Mobile Border Surveillance Systems

Mobile border surveillance systems are capable of collecting surveillance data from various locations, because the surveillance platform can physically be moved to meet changing mission needs. A description of each of the mobile border surveillance systems follows:

- Mobile Video Surveillance System (MVSS) uses mobile video recording units on platforms that can be moved to provide the best visual range for surveillance of several miles. MVSS provide day and night surveillance images that allow the user or operator to determine if there are items of interest or suspicious criminal activities occurring with the area of coverage and to provide situational awareness to the interdicting Border Patrol Agent.
- Mobile Surveillance Capability (MSC) uses truck-mounted mobile video recording units with cameras and radar mounted to extended masts that allow on-board monitoring of surveillance images by an attending user. MSC covers a range of several miles under optimal conditions. MSC is deployed primarily in rural remote areas or other areas where no fixed surveillance technologies are deployed.
- Agent Portable Surveillance System (APSS) is a surveillance suite that includes cameras with a visual range for surveillance of several miles and ground radar that can be carried and used by Border Patrol Agents in areas where fixed and vehicle-mounted solutions are not feasible or appropriate.
- Ultra-Light Aircraft Detection (ULAD) is a mobile radar system that is being tested to detect and track small, low, or slow flying aircraft with a small radar cross section, known as ultra-light aircraft, in remote areas along U.S. borders. The ULAD system increases and enhances operators' ability to identify suspicious small aircraft[2] so that CBP can monitor possible smuggling routes and make an interdiction. The ULAD system tracks aircraft from entry to either landing or exiting the U.S. when aerial assets are not within response range. ULAD transmits

[2] Small aircraft refers to the ultra-light aircraft, which are essentially hang-gliders with an engine and a prop.

radar sensor data to the Air and Marine Operations Center (AMOC) in Riverside, CA and Border Patrol Sector Dispatch Centers. The AMOC also has remote control capability for the detection units.

Fixed Border Surveillance Systems

Fixed border surveillance systems are capable of collecting surveillance data from a dedicated location. A description of each of the fixed border surveillance systems follows:

- Tethered Aerostat Radar System (TARS) uses the aerostat (a large unmanned blimp or balloon) as a stationary airborne platform for surveillance radar. TARS detects and monitors low-altitude aircraft and vessels along the U.S.-Mexico border, the Straits of Florida, and a portion of the Caribbean in support of the Counter-Narcotics Program with the Department of Defense (DOD). The program's primary mission is to provide persistent, long-range, detection and monitoring of low-level air, maritime, and surface narcotics traffickers using radar detection. There are currently eight operational sites in the continental United States and Puerto Rico.[3] Some TARS are equipped with a video camera capable of assisting CBP users in detecting and tracking pedestrian and vehicular traffic; other sites monitor maritime traffic and relay CBP communications to facilitate interagency operations.
- Integrated Fixed Tower (IFT) sensor suites include towers with mounted day and night cameras and radar that can be monitored from a local CBP Border Patrol sector facility.
- Block 1 and Northern Border Remote Video Surveillance System (RVSS) provide automated day and night wide-area surveillance along the U.S. border using multiple color cameras and thermal infrared detection video cameras. CBP uses RVSS to detect and track illegal entries. The sensor images are transmitted via a dedicated communications system to a CBP facility where the information is processed and displayed.
- The Intelligent Computer Assisted Detection (ICAD) system operates a network of underground sensors and cameras installed along the U.S. border that detects the presence or movement of individuals and relays that information to U.S Border Patrol Sector Headquarters. ICAD records the date, time, and location of the activity, as well as details input by the Border Patrol Agent investigating the incident. Border Patrol Agents input details including name, date of birth, document number, license plate number, and other biographic data about individuals encountered through ICAD detections. The sensor data is stored and can be retrieved by date, time, or the PII that is included in the incident details.
- Law Enforcement Technical Collection (LETC) intercepts radio communications on HF, VHF, and UHF frequencies. LETC operators only collect radio communications in compliance with applicable laws, directives, and policies. CBP officials make notes of suspicious radio chatter including frequency used, location of transmission, code names, and code words to log suspicious

[3] The eight operational sites are: Yuma, AZ; Ft. Huachuca, AZ; Deming, NM; Marfa, TX; Eagle Pass, TX; Rio Grande City, TX; Cudjoe Key, FL; and Lajas, PR.

activity. No log entry is created if the activity is deemed not to be of law enforcement interest.

LETC log entries are retrieved by date, time, frequency, and location of the event. CBP does not retain the transmitted audio unless it is used in support of an ongoing law enforcement activity.

LETC supports the prevention of unauthorized entries by persons; interdiction of smuggled, hazardous material, and contraband; and it assists investigative efforts using a risk-based strategy.

The combination of fixed and mobile surveillance systems supports CBP's persistent and situational surveillance of the U.S. border at and between ports of entry. Sensor information may be relayed to a Border Patrol sector station, Headquarters, port of entry, or users at a fusion center to coordinate a response when available and where necessary to respond. Sensor information is displayed to authorized users at these locations based on their assigned duties and need to know.

CBP is better able to respond to and coordinate its interdictions and law enforcement responses to events at or near the border using the sensor technologies described in this PIA. CBP uses the Land Mobile Radio Network (LMR) to coordinate its response. LMR is a CBP internal radio network responsible for providing tactical communications, operational planning, radio network control services, and investigative information and intelligence services to support CBP operations, port of entry inspections, and other law enforcement activities as required. LMR records radio conversations between Border Patrol Agents in the field and dispatch operators.[4] The CBP Office of Internal Affairs uses audio logs to retrace the activity when investigating incidents involving Border Patrol Agents. The audio logs are kept for a period of seven days and then overwritten by the system unless the information is used in support of ongoing law enforcement investigations by the appropriate federal agency.

Border Patrol Agents may process the apprehension using a mobile processing center or at the sector station when CBP encounters individuals away from a port of entry. BSS users copy the video images and audio recordings from BSS to an archive to be used as law enforcement records and as evidence in any subsequent proceedings during processing. If an incident results in prosecution the authorized BSS users retrieve the BSS recording by the date, time, and device number and provide it to the investigating or prosecuting agency along with the related case file information. All physical transfers of data are recorded on a chain of custody form completed by the user performing the transfer.

Section 1.0 Authorities and Other Requirements

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

The BSS represent a reassessment of SBInet as authorized under the Secure Fence Act of 2006 and implementing regulations.[5] CBP uses BSS to perform its law enforcement missions under the

[4] Other federal and state agencies leverage this technology including the U.S. Department of Justice, U.S. Department of Interior, and the Massachusetts Criminal Justice Information Service to record and transport their radio conversations. However, the recordings are logically segregated from CBP recordings, and each agency does not have access to another agency's recordings.
[5] Pub. L. 109-367, 8 U.S.C. § 1707 Note and 8 CFR 287.

Immigration and Nationality Act of 1952, as amended, and other pertinent provisions of the immigration laws and regulations,[6] as well as pertinent provisions of the customs laws and regulations.[7] CBP collects information through BSS in conformance with the Electronic Communications Privacy Act of 1986, as amended, and the Communications Act of 1934, as amended.[8]

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

Audio and video recordings in BSS are not retrieved from the device or archive storage using a personal identifier, and therefore, do not constitute a system of records under the Privacy Act of 1974. However, video and audio recordings associated with an individual in a case file and retrieved by a personal identifier are covered under the associated system of records. For example, video associated with a law enforcement activity may be linked to PII maintained in reports and records residing in the associated case file system of records, including DHS/CBP-011 U.S. Customs and Border Protection TECS;[9] DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE);[10] DHS/CBP-017 Analytical Framework for Intelligence System (AFI);[11] or DHS/ALL-020 Department of Homeland Security Internal Affairs.[12]

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

The BSS projects described above are in various stages of the system development life cycle. System Security Plans (SSP) have been completed for Block 1, Northern Border Remote Surveillance System, and Agent Portable Surveillance Systems. All others have system security plans in development.

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

No. CBP is developing a retention schedule for archive storage of BSS data for NARA according to the retention procedures described in 5.1, below.

---

[6] Pub. L. 82-414. *See*, *e.g.*, 8 U.S.C. §§ 1225 and 1357.
[7] *See*, *e.g.*, 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, and 1595a(d).
[8] 18 U.S.C. § 2510 *et seq*; 47 U.S.C. § 151 *et seq*.
[9] U.S. Customs and Border Protection TECS SORN, 73 FR 77778 (Dec. 19, 2008), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.
[10] DHS/ICE-011 - Immigration and Enforcement Operational Records System (ENFORCE), 75 FR 23274 (May 3, 2010), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2010-05-03/html/2010-10286.htm.
[11] DHS/CBP-017 Analytical Framework for Intelligence System, 77 FR 13813 (June 7, 2011), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm.
[12] DHS/ALL-020 - Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2014-04-28/html/2014-09471.htm.

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

The BSS does not collect information covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

BSS collect various types of data that may include PII. Some of the information collected is stored and can be retrieved. Collected information includes:

Video recordings and still images: BSS use mobile and ground fixed cameras to routinely monitor remote border areas for suspicious activity or an unexpected presence. Some video cameras have night vision or thermal imaging capability for monitoring an area at night. The video records and tracks the presence of people illegally crossing the border and entering U.S. territory. Video recordings and still images derived from video recordings may become associated with PII in a case file.

Radio frequency transmissions: BSS intercepts radio communications on HF, VHF, and UHF frequencies used by terrorists and transnational criminal organizations for illicit activities. CBP officials make notes of suspicious radio chatter, including frequency used, location of transmission, code names, and code words to log suspicious activity. Log entries are not created if the activity is deemed not to be of law enforcement interest. LETC log entries are retrieved by date, time, frequency, and location of the event. CBP does not retain the transmitted audio unless it is used in support of ongoing law enforcement operations.

LMR: CBP logs all audio transmissions between Border Patrol Agents and dispatch operators to retrace the activity when investigating incidents involving CBP agents. An audio logging recorder is active at all CBP sector offices and the National Law Enforcement Communication Center (NLECC). The audio logging recording is used by Internal Affairs. Audio logs are kept for a period of seven days and then overwritten by the system unless the information is used in support of ongoing law enforcement investigations by the appropriate federal agency.

Under Ground Sensors: ICAD reads data sent by underground sensors to detect persons or vehicular movement across and along the border and relays the data to a Border Patrol station for a response. ICAD sensor data is stored in ICAD with associated incident details including PII about the persons encountered (name, phone number, address, make and model of vehicle, license plate number, driver's license number, etc.). The data collection, storage, usage, and retention is documented in the forthcoming ICAD SORN.

Radar: CBP collects radar data from MSC, APSS, ULAD, and TARS to detect and interdict aircraft, vehicles, vessels, and other conveyances in the border area and drug trafficking transit zones, such as the adjacent portions of the Caribbean Sea. This radar data does not contain PII, but may be used to locate and apprehend an individual illegally crossing the border. CBP uses MSC and APSS to detect individuals and conveyances moving over ground in remote areas, which may lead to an interdiction. ULAD detects the presence of small aircraft flying along the border. TARS provides persistent, long range, radar for detection and monitoring of low-level air, maritime, and surface contacts along the U.S.-Mexico border, the Straits of Florida, and adjacent portions of the Caribbean sea.

When BSS data is needed as evidence for prosecution, a BSS user retrieves the recorded incident information from the respective border surveillance system or archive based on the case file information (time/date/tower location number) and saves it to a DVD. CBP then controls the BSS data along with the case file information according to its "chain of custody" handling procedures for evidence.

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

CBP collects raw video, photograph, audio, ground sensor, and radar data using BSS in rural and populated areas at or near the U.S. border. Additionally, TARS collects radar data in adjacent portions of the Caribbean Sea.

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

No. BSS does not use information from public or commercial sources. Also, the BSS have no connections to public or commercial sources, such as the internet.

2.4 Discuss how accuracy of the data is ensured.

CBP captures BSS video, images, audio, ground sensor, and radar data in real-time to maintain a factual record of events. Accuracy is ensured by instructing users to adjust the recording equipment to increase a video image's resolution or sound quality from a microphone. CBP trains BSS operators to properly evaluate and ascertain which data is relevant and necessary to accomplish CBP's border securing mission before copying data off of a device or archiving an incident. This training ensures that the subject of the video or audio collection is within the scope of the defined mission. The alignment of the collection activity within the scope of the mission parameters becomes a critical factor for determining accuracy and relevance because the subject may be determined by an event or circumstance (such as presence at a "drop zone") instead of by identity. CBP also follows chain of custody procedures to ensure the integrity of the records when records are used as evidence and therefore linked directly to a case or person.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that BSS may capture information about individuals or activities that are beyond the scope of CBP's authorities. Video cameras can capture individuals entering places or engaging in activities as they relate to their daily lives because the border includes populated areas. For example, BSS may collect video of an individual entering a doctor's office, attending public rallies, social events or meetings, or associating with other individuals.

Mitigation: Cameras, radar, and other BSS are oriented toward the border and away from communities and places of worship and commerce frequented by local residents, when operationally feasible. While BSS records lawful activity at or near the border, these recordings are automatically overwritten unless an authorized BSS user determines the recording is needed for an approved purpose. Specifically, CBP copies and retains information from BSS only when it is relevant to an active case file for law enforcement or border security purposes. Additionally, CBP does not associate the recorded video or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation.

Privacy Risk: LETC users may listen to or record radio frequency communications between individuals engaged in activities with no law enforcement nexus.

Mitigation: CBP intercepts radio frequency communications near the border that may include communications with no law enforcement nexus; however, CBP is subject to applicable laws, directives, and policies so that log entries are not created and audio is not retained if the activity does not have a law enforcement nexus. CBP officers and agents receive training that addresses awareness of sensitivities arising in conversations, as well as determining associations between the topic of a conversation and a mission purpose. As with any information acquired as part of official responsibilities, CBP officers and agents may not disclose any information collected, unless authorized in accordance with DHS and CBP policy, and remain subject to the CBP Code of Conduct and relevant disciplinary procedures for any violation.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

CBP primarily uses information obtained from BSS to enhance border security and interdiction operations at the border. BSS users track the movement of individuals and incidents near the border and dispatch available Border Patrol Agents to provide operational support. CBP uses video surveillance to monitor a particular individual or location as part of a law enforcement investigation and may use the collected images as evidence in criminal proceedings in the event the individual is arrested. CBP uses radar and ground sensor data to detect and interdict persons illegally crossing the border. CBP's Internal Affairs uses LMR audio recordings to retrace events when an incident occurs with a Border Patrol Agent. LETC users note suspicious radio chatter to detect illegal activity at the border. CBP shares BSS information with coordinating agencies to assist in an interdiction or operation, as appropriate and

described by the routine uses of the respective SORNs that govern the case file or investigative report (e.g., TECS, Automated Targeting System-Targeting Framework, E3/ENFORCE).

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

No.

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

No.

3.4 Privacy Impact Analysis: Related to the Access, Uses, and Disclosure of Information

Mitigation: CBP employees only use BSS in compliance with applicable laws, policies, and directives. CBP trains users about appropriate collection and use procedures before providing access to a particular system. Failure to comply with these guidelines is a violation of CBP's Code of Conduct and may subject an employee to disciplinary action, including termination of employment or prosecution.

Risk: There is potential risk of unauthorized access, use, or disclosure of video or audio recordings from BSS.

Mitigation: Access to BSS is limited to those specific CBP employees that must use the systems as part of their assigned duties. Equipment use is tracked and monitored for accountability and authorized users and system administrators are the only persons with access to the systems and surveillance data. All equipment and archives are stored in secure facilities with limited access. CBP does not share the information with any other component or agency unless it becomes evidence in a law enforcement investigation. Information sharing is compliant with the routine uses of the respective SORNs.

Section 4.0 Notice and Consent

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

All persons entering the U.S. at and between the ports of entry are subject to monitoring and data collection for operational and situational awareness. CBP posts signs at ports of entry to notify

individuals of the monitoring and information collection requirements. CBP conducted an environmental assessment process prior to the implementation of the Integrated Fixed Towers that involved public hearings to raise awareness of the program and give the public an opportunity to comment on the location of fixed cameras and their use. This PIA also serves to inform the public generally of the presence of surveillance devices at the border and the use of these devices to detect and support the apprehension of persons crossing the border illegally.

CBP does not provide advanced notice for individuals encountered between ports of entry because entering the U.S without coming through a port of entry is illegal. It is logistically impracticable for CBP to give prior notice to persons seeking to cross the border at other than a port of entry; persons seeking to cross the border illegally are informed that their activities in the border area may be monitored and captured for use to enforce the law through the notice provided in this PIA and the associated SORNs.

4.2 Privacy Impact Analysis: Related to Notice

Risk: There is a risk that collected images or activities at the border either at or between the ports of entry may include innocent persons or persons who are complying with the law and who have not received notice or provided consent.

Mitigation: Notice for persons at the ports of entry is provided at the ports. Notice for persons in the border area between the ports of entry is found in this PIA. As described above, CBP conducted public meetings before installing the Integrated Fixed Towers to allow for extended notice and comment from persons living in the immediate vicinity of the tower emplacements.

CBP does not obtain consent to use information pertaining to persons crossing the border as it is obliged by statute to ensure the security of the border and to determine the identity and citizenship of all persons crossing the border. CBP signage at the ports of entry informs persons of the video capture and its intended use. CBP recognizes that residents and visitors in areas proximate to the ports of entry and the border may have their images captured incidentally. CBP mitigates this risk by strictly controlling the collection, use, and retention of information through BSS. Information that is not collected for a law enforcement purpose is deleted and is not used.

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

CBP does not provide opportunities for consent to monitoring and capturing an individual's image, radio frequency transmissions, or travel in the border areas due to the law enforcement and border security nature of the data captured through BSS surveillance activities at and between the ports of entry. Information collected by CBP that does not pertain to a law enforcement activity is deleted and is not used.

Section 5.0 Data Retention by the project

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

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

BSS equipment may temporarily retain recordings or directly transmit them to an archive. Both the device and the archive overwrite data after a set period of time, as described below unless the recording is associated with a case file. CBP retains recordings associated with a case file for the retention period of the case file, including proceedings associated with a case file. The retention schedule of the applicable case management system will apply to the associated BSS information once a case has been closed.

Video recordings are stored on the device for varying amounts of time, typically between seven and 30 days before being overwritten. CBP copies the video to an archive and has proposed retention of video recordings for 45 days in an archive before being purged, unless the video is useful for training purposes or is associated with a case file. CBP may keep recordings that are useful for training purposes for up to one year.

LMR audio logs are retained for seven days before being overwritten unless it is needed for and associated with a law enforcement investigation or incident.

Ground sensor data is retained along with incident details according to the ICAD SORN retention period, which is proposed for up to 15 years.

Radar data are not retained unless they are associated with a case file.

Radio frequency transmissions are not retained unless they are used in support of ongoing law enforcement operations and associated with a case file.

5.2 Privacy Impact Analysis: Related to Retention

Risk: There is the risk that surveillance video and recordings may be retained in BSS for a longer period than required by the purpose for which the video and images were collected.

Mitigation: CBP automatically overwrites video that is not needed and identified for an authorized training purpose or for a specific law enforcement investigation or incident to minimize the risk of excessive data retention. Videos used for training are marked and purged after one year. All other recordings that are not associated with a person will be automatically purged within 45 days. CBP identifies and associates recordings with persons to pursue its several law enforcement missions at the border; in these matters the recordings are maintained in association with the respective case management system holding the associated law enforcement matter about the person. CBP maintains recordings in these instances in accordance with the retention period for the respective case management system.

Section 6.0 Information Sharing

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

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

CBP shares non-PII radar data with the DOD as part of the joint Counter-Narcotics Program. When CBP identifies a possibly illicit radio frequency transmission, CBP provides non-PII notes from the transmission (frequency band, time, date, and location) to the Federal Communications Commission (FCC) and the Drug Enforcement Agency (DEA) for their law enforcement purposes.

CBP does not ordinarily share video or audio outside of CBP. Rather, CBP typically shares information derived from BSS with other law enforcement agencies assisting CBP in an interdiction or law enforcement operation. For example, a BSS user watching a video camera may relay "three suspects are running towards a blue truck near the intersection of X and Y" with local law enforcement on the scene to coordinate the interdiction. CBP provides the video or audio extract as part of the case file shared with federal law enforcement (e.g., Department of Justice) in the event surveillance information results in an arrest and subsequent prosecution.

CBP shares audio or video recordings along with other case file information from a system of records consistent with the Privacy Act of 1974 and the routine uses in the applicable SORN(s) when an audio or video recording from BSS is associated with a system of records. CBP documents the disclosure on a Form DHS-191 when BSS information is shared in conjunction with PII from a system of records. CBP conditions the disclosure to the receiving agency on:

1. the receiving agency's use being consistent with the purpose for collection;
2. the sharing being consistent with a statutory or published routine use; and
3. the receiving agency's acceptance of the restriction barring unauthorized dissemination outside the receiving agency.

These conditions are stated in the written authorization provided to the receiving agency and represent the constraints on the use and disclosure of the information at the time of the disclosure.

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

CBP may disclose the information pursuant to the routine uses outlined in the appropriate case file SORN when BSS information is associated with PII in a system of records. For example, video may be shared with local law enforcement to assist with a law enforcement investigation if the video is associated with a case file in:

- TECS pursuant to routine use G, which states, "To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines

that the information would assist in the enforcement of civil or criminal laws."[13]

- Internal Affairs pursuant to routine use G, which states, "To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure."[14]
- ENFORCE pursuant to routine use G, which states, "To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure."[15]
- AFI[16] pursuant to routine use H, which states, "To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, agreement, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws. This routine use applies only to finished intelligence products."[17]

Normally, the requesting agency seeks the information through a Request for Information (RFI), to which CBP responds. The terms of this response discuss the need and authority identified by the requesting agency for use of the information; it then relates those terms to the purpose for which CBP collected and maintains the information under its specific SORN (for example, a DEA request for information pertaining to drug trafficking maintained in a law enforcement case management system). The response notes that CBP requires consultation with respect to further dissemination of the shared information beyond the receiving agency so as to ensure accountability for the collected information.

6.3 Does the project place limitations on re-dissemination?

Yes. CBP only shares video or audio when the requesting agency has an official need to know and agrees to limit re-dissemination by first obtaining approval from CBP, regardless of whether it is associated with a system of records. CBP responds to requests for information or assistance by providing

[13] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR, 77778 (Dec. 19, 2008).
[14] DHS/ALL-020 Department of Homeland Security Internal Affairs 79FR 23361 (April 28, 2014).
[15] DHS/ICE-011Immigration and Enforcement Operational Records System (ENFORCE) 75 FR 23 274 (May 3, 2010).
[16] DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) PIA, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf.
[17] DHS/CBP-017 Analytical Framework for Intelligence System (AFI) 77 FR 33753 (June 7, 2012).

a written response to document the terms and conditions of use.

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

Video or audio associated with a system of records that is shared outside of the Department is tracked through the use of the DHS-191, Accounting of Disclosure Form. The form requests the date, nature, purpose of each disclosure, and the name and address of the individual agency to which disclosure is made. *Ad hoc* requests not associated with information from a system of records must be approved by the appropriate Program Director and documented locally.

6.5 Privacy Impact Analysis: Related to Information Sharing

Risk: There is the risk that PII from BSS may be shared inappropriately with external organizations.

Mitigation: The same limitations on the use of the information that are in place for CBP and DHS also apply to the outside entity when sharing information with third parties. CBP restricts sharing or access to BSS data based on "need to know" criteria, which requires the receiving entity to demonstrate a need for the data that is compatible with the use for which it was originally collected before the video or audio is disseminated. Likewise, the receiving entity must provide assurances that the data will be safeguarded in a manner consistent with CBP/DHS policy and practice and that the receiving agency will not disclose any shared data without the express prior written permission of CBP.

CBP does not currently have any arrangements to share BSS data associated with an individual in an automated fashion. CBP will develop a written arrangement (e.g., Memoranda of Understanding (MOU) or Information Sharing Access Agreement (ISAA)) that would specify with particularity all terms and conditions that govern the use of the data in the event that such a recurring sharing arrangement is contemplated between CBP and an agency outside DHS. CBP would review the written arrangement and verify that the outside entity conformed to CBP's use, security, and privacy considerations before releasing information.

Section 7.0 Redress

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

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

Much of the data in BSS is law enforcement sensitive and generally unavailable for access by the public. However, individuals may request information contained in BSS through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and, when applicable, the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)).

Individuals seeking notification of, and access to any record contained in BSS, in a system of

records containing data from BSS, or seeking to contest its content may gain access by filing a FOIA or Privacy Act request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, D.C., 20229-1181
Fax Number: (202) 325-0230

Most BSS data is not accessible under the Privacy Act of 1974 because BSS data on the device or in an archive is not retrievable by personal identifier. However, CBP provides individuals access to BSS data according to the applicable SORN when CBP associates BSS data with an individual by linking it to a case file in a system of records. There may be occasions when BSS information is covered by a SORN and DHS exempts the information from individual access or amendment provisions of the Privacy Act. This occurs if access to the data could inform the subject of an investigation of the existence of the investigation or reveal investigative interest on the part of DHS or another agency. Access to the CBP-held records could also be denied if such access might permit the individual who is the subject of a record to impede an investigation, tamper with witnesses or evidence, and avoid detection or apprehension. In other cases individuals may be able to gain access to the data pertaining to them.

CBP reviews all such requests on a case-by-case basis, notwithstanding the applicable exemptions. CBP may waive the applicable exemption and provide access to BSS data if it does not interfere with or adversely affect the national security of the United States or activities related to any investigations associated with the BSS data.

Further, individuals may contest information collected through BSS if it is used as evidence in any immigration or criminal proceedings that result from the encounter.

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

Individuals may contest information collected through BSS through any immigration or criminal proceedings that result from the encounter. The individual may file a Privacy Act amendment request if the BSS data is associated with a system of records.

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

CBP is providing notice to the public through this PIA, the applicable SORNs, and through the FOIA section on www.cbp.gov.

7.4 Privacy Impact Analysis: Related to Redress

Risk: There is the risk innocent individuals may suffer negative effects if their images are erroneously associated with a crime without the ability to correct it.

Mitigation: CBP does not use surveillance images to identify an individual, but instead to detect

and interdict suspected criminal activity. An individual can only be linked to an image if the BSS data leads to an apprehension, subsequent identification, and association with the case file. The individual may contest the association through the subsequent immigration or criminal proceeding if he or she is erroneously associated with BSS data.

Section 8.0 Auditing and Accountability

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

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

Handling the information that is collected by the BSS is governed by standard operating procedures and policies. Only authorized users have the ability to extract materials from the systems. CBP mitigates the risk of misuse of data collected by, and accessed through BSS by maintaining audit trails, including (at a minimum): user name, access date and time, and functions and records addressed. CBP also requires users to conform to appropriate security and privacy policies, follow established rules of behavior, and receive adequate training regarding the security of the system.

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

All BSS users undergo initial security awareness training and complete the DHS online security awareness-training course and a privacy awareness course on an annual basis.

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

All CBP employees who operate BSS receive training on proper use of the systems and handling of any evidentiary data that may be extracted from the system. All first time users must take a two-day Security Awareness Training provided on the surveillance systems. Users may only request an access account after they have completed the two-day training. The trained user submits account creation forms requiring him or her to provide proof of security awareness training and sign an agreement to abide by the system rules of behavior. The system maintains a log of activities for auditing purposes. CBP program managers and supervisors must authorize each employee to perform certain functions related to BSS. Only authorized personnel are able to delete or add records before or after storage in an archive. For example, while each monitoring user has the ability to operate the surveillance cameras and save eventful surveillance video to the archive server, only the on-duty Video Retention Coordinator may delete video files. Users may not remove or download data from the archive server without authorization and in conjunction with assistance from the aforementioned Video Retention Coordinator. These precautions not only safeguard the data but also ensure the integrity of the information for when it is necessary to be used as evidence.

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

All information sharing and MOUs concerning the sharing of PII, including those related to BSS, are created by the operational owner of the system and are sent to the CBP Privacy Officer and Office of Chief Counsel for review and to the DHS Privacy Office for final concurrence before being approved and signed.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
U. S. Customs and Border Protection
(202) 344-1610

Douglas Harrison
Associate Chief, Office of Border Patrol
U.S. Customs and Border Protection
(202) 344-2050

Sonia Padilla
Executive Director, Program Management Office
U.S. Customs and Border Protection
Office of Technology Innovation and Acquisition
(571) 468-7500

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Privacy Impact Assessment
for the

Border Searches of Electronic Devices

August 25, 2009

Contact Points
Thomas S. Winkowski
Assistant Commissioner, Office of Field Operations
U.S. Customs and Border Protection
(202) 344-1620

Kumar C. Kibble
Acting Director, Office of Investigations
U.S. Immigration and Customs Enforcement
(202) 732-3000

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
U.S. Department of Homeland Security
(703) 235-0780

Abstract

With changes in technology over the last several decades, the ability to easily and economically carry vast amounts of information in electronic form has risen dramatically. The advent of compact, large capacity, and inexpensive electronic devices, such as laptop computers, thumb drives, compact disks (CD), digital versatile disks (DVD), cell phones, subscriber identity module (SIM) cards, digital cameras, and other devices capable of storing electronic information (hereinafter "electronic devices") has enabled the transportation of large volumes of information, some of which is highly personal in nature. When these devices are carried by a traveler crossing the U.S. border, these and all other belongings are subject to search by the U.S. Department of Homeland Security (DHS) to ensure the enforcement at the border of immigration, customs, and other federal laws. In particular, U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) may conduct border searches of such electronic devices as part of CBP's mission to interdict and ICE's mission to investigate violations of federal law at and related to the Nation's borders. CBP Officers and ICE Special Agents conduct border searches of electronic devices to determine whether a violation of U.S. law has occurred.

Overview

There are two basic privacy concerns at the heart of DHS searching electronic devices at the border. The first is the propriety of the border search, as in whether the search is lawful under U.S. law. 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 below.[1]

The second and more central privacy concern is the sheer volume and range of types of information available on electronic devices as opposed to a more traditional briefcase or backpack. In the past, someone might bring a briefcase or similar accessory across the border that contains pictures of their friends or family, work materials, personal notes or journals, or any other type of personal information. Because of the availability of electronic information storage and the capacity for comfortable portability, the amount of personal and business information that can be hand-carried by a single individual has increased exponentially. Where someone may not feel that the inspection of a briefcase would raise significant privacy concerns because the volume of information to be searched is not great, that same person may feel that a search of their laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices.

At the same time that individuals seek to lawfully transport electronic information with no link to criminal activity across the border, criminals attempt to bring merchandise contrary to law into the United States using the same technology. The use of electronic devices capable of storing information relating to criminal activities has been established as the latest method for smuggling these materials. As the world of information technology evolves, the techniques used by CBP and ICE and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals using new technologies in the

[1] *See, e.g.,* 19 U.S.C. §§ 482, 1461, 1496, 1499, 1581-1582; *see generally United States v. Flores-Montano,* 541 U.S. 149 (2004); *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985).

perpetration of crimes. Failure to do so would create a dangerous loophole for criminals seeking to import or export merchandise contrary to law.

Because of the unique privacy concerns raised by the border search of electronic devices, CBP and ICE have conducted this Privacy Impact Assessment (PIA) to enhance public understanding of the authorities, policies, procedures, and privacy controls related to these searches. This PIA discusses DHS's general border security mission, definitions of commonly used terms, and the parameters of border searches conducted by CBP and ICE. This PIA details the border search process as it pertains to electronic devices, concentrating on why CBP and ICE conduct searches, how CBP and ICE handle electronic devices, and the policies and procedures in place to protect individuals' privacy. This PIA concludes with a privacy risk and mitigation analysis of those policies and procedures based on the DHS's Fair Information Practice Principles.[2]

DHS's Border Security Mission

DHS is charged with ensuring compliance with federal laws at the border including those preventing contraband, other illegal goods, and inadmissible persons from entering or exiting the United States. DHS's border authorities permit the inspection, examination, and search of vehicles, persons, baggage, and merchandise to determine if the merchandise is subject to duty or being introduced to the U.S. contrary to law, and to ensure compliance with any law or regulation enforced or administered by DHS. Accordingly, all travelers entering the United States must undergo DHS customs and immigration inspection to ensure that they are legally eligible to enter (as a U.S. citizen or otherwise) and that their belongings are not being introduced into the U.S. contrary to law. It is not until those processes are complete that a traveler, with or without his belongings, is permitted to enter the United States.

During the immigration process, travelers are subject to an examination to determine alienage, nationality, and admissibility into the United States. During the customs inspection, travelers are subject to border search for merchandise, regardless of status in the United States. Both the examination and search may be conducted without a warrant and without suspicion.[3] Long-standing customs authorities allow for border searches to be performed with or without suspicion that the merchandise being searched may be in violation of U.S. law or may contain evidence of such a violation.[4] Significantly, the Executive's plenary authority to conduct border searches derives from statutes passed by the First Congress.[5] The Supreme Court has repeatedly described this authority as having an "impressive historical pedigree,"[6] that underscores the inherent right of the sovereign to protect its "territorial integrity."[7] Under DHS authorities to conduct border searches, travelers' electronic devices are equally subject to search as any other belongings because the information contained in them may be relevant to DHS's customs and immigration inspection processes and decisions. While the terms "merchandise" and "baggage" are used, the courts have interpreted border search authorities to extend to all of a traveler's

---

[2] *See The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008 (http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).
[3] *See United States v. Ramsey*, 431 U.S. 606 (1977). *See also* Act of July 31, 1789, ch 5, 1 Stat. 29.
[4] *See United States v. Ramsey*, 431 U.S. 606 (1977). *See also* Act of July 31, 1789, ch 5, 1 Stat. 29.
[5] Act of Aug. 4, 1790, 1 Stat. 164.
[6] *See U.S. v. Villamonte-Marquez*, 462 U.S. 579, 585 (1983).
[7] *See Flores-Montano*, 541 U.S. at 153.

belongings, including electronic devices and the information in such devices.[8] In addition to searches conducted to ensure merchandise is not being introduced into the U.S. contrary to law, the authorities for these searches also allow for the review of information relating to the admissibility of persons into the United States under federal immigration law.

DHS's border search authorities are derived from those exercised, prior to the homeland security reorganization in 2003, by the U.S. Customs Service (USCS) and the Immigration and Naturalization Service (INS). Those agencies were merged into DHS and reorganized into the Customs Service – later renamed CBP, which retained the inspectional and patrol functions of USCS and INS; and ICE, which retained the investigative components of USCS and INS. CBP and ICE continue to hold the border search authorities previously exercised by USCS and INS. CBP, as the interdictory agency, and ICE, as the investigative agency, now work hand-in-hand at the border to set forth a seamless process for the international traveler.

Border Searches in Support of CBP and ICE Law Enforcement Missions

As the Nation's law enforcement agencies at the border, CBP interdicts and ICE investigates a range of illegal activities such as child pornography; human rights violations; smuggling of drugs, weapons, and other contraband; financial and trade-related crimes; violations of intellectual property rights and law (e.g., economic espionage); and violations of immigration law, among many others. CBP and ICE also enforce criminal laws relating to national security, terrorism, and critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.

In the course of their daily practices, CBP Officers and ICE Special Agents may interview travelers undergoing inspection at the border and/or conduct border searches of travelers and their belongings.[9] In some cases, CBP and/or ICE may search a traveler because he is the subject of, or person-of-interest in, an ongoing law enforcement investigation and was flagged by a law enforcement "lookout" in the CBP enforcement system known as TECS.[10] If questions regarding the admissibility of an individual or his or her belongings cannot be resolved at the primary inspection station, CBP may elect to conduct a more in-depth inspection of the traveler (referred to as "secondary inspection"). At any point during the inspection process, CBP may refer the traveler and his belongings to ICE for a search, questioning, and for possible investigation of violations of law. ICE has concurrent border search authority with CBP and may join or independently perform a border search at any time.

In many instances, CBP and ICE conduct border searches of electronic devices with the knowledge of the traveler. However, in some situations it is not practicable for law enforcement reasons to inform the traveler that his electronic device has been searched.

---

[8] *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008), *cert. denied*, 129 S.Ct. 1312 (Feb. 23, 2009); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006); and *United States v. Roberts*, 274 F.3d 1007 (5th Cir. 2001).

[9] Travelers arriving in the United States at a port of entry must go through CBP inspection where CBP has two missions, which are often interdependent: (1) to ensure the traveler is legally admissible to the United States; and (2) to ensure all items accompanying the traveler are permitted legal entry into the United States.

[10] *See* the Privacy Act System of Records Notice, DHS U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008, 73 FR 77778.

Frequently Used Terms

The following terms are used throughout this PIA.

- A detention occurs when CBP or ICE determines that the devices need to be kept for further examination to determine if there is probable cause to seize as evidence of a crime and/or for forfeiture. This is a temporary detention of the device during an ongoing border search. Many factors may result in a detention, for example, time constraints due to connecting flights, the large volume of information to be examined, the need to use off-site tools and expertise during the search (e.g., an ICE forensic lab), or the need for translation or other specialized services to understand the information on the device. In a detention, CBP or ICE will keep either the original device (e.g., the laptop) or an exact duplicate copy of the information stored on the device, so as to allow the traveler to proceed with the original device. Once the border search has concluded, the device will be returned to the traveler unless there is probable cause to seize the device. Any copies of the information in the possession of CBP or ICE will be destroyed unless retention of the information is necessary for law enforcement purposes and appropriate within CBP or ICE Privacy Act systems of records.

- A seizure occurs when CBP or ICE determines there is probable cause to believe a violation of law enforced by CBP or ICE has occurred based on a review of information in the electronic device during the border search or based on other facts and circumstances.

- A retention occurs when CBP or ICE stores information from a device in any of their recordkeeping systems. A retention typically occurs when an electronic device is detained and the border search reveals information relevant to immigration, customs, or other laws enforced by DHS. For example, the traveler may appear to be permitted legal entry into the United States as a visitor, but a file on his laptop may evidence his true intent to secure employment in the United States, thus making him inadmissible.

- Computer Forensic Agents (CFAs): CBP Officers and ICE Special Agents may perform border searches on electronic devices; however, within ICE, only those Special Agents trained by ICE and certified as CFAs are permitted to extract information from electronic devices for ICE evidentiary purposes. CFAs are specially trained on information technology, evidentiary, and legal issues involving the search, analysis, duplication, and seizure of electronic information. Within ICE, only CFAs are permitted to make duplicate copies of electronic devices during a search to ensure secure and accurate duplication of the information, and the integrity of the information (original and copy) and the electronic devices. CFAs are also trained in the proper and secure destruction of electronic information.

- Demand for Assistance: During a border search, ICE and CBP have specific statutory authority to demand assistance from any person or entity.[11] For searches of electronic devices, CBP or ICE may demand technical assistance, including translation or decryption, or

[11] *See* 19 U.S.C. § 507.

specific subject matter expertise that may be necessary to allow CBP or ICE to access or understand the detained information.

Process

Travelers arriving at a port of entry must go through primary inspection, where a CBP Officer checks the traveler's documentation and determines the traveler's admissibility to the United States. During primary inspection, the CBP Officer may determine, through his observations or through an alert indicated on the primary inspection computer screen, that the traveler warrants further examination and thus will refer the traveler to secondary inspection. Travelers are typically referred to secondary inspection to resolve immigration, customs, or other law enforcement matters. At secondary inspection, a CBP Officer or ICE Special Agent may ask the traveler questions and inspect the traveler's possessions to detect violations or evidence of violations of law. This border search may include examination of documents, books, pamphlets, and other printed material, as well as computers, storage disks, hard drives, phones, personal digital assistants (PDAs), cameras, and other electronic devices. Referrals for secondary examination may also be the result of a random compliance measurement selection through a system referred to as COMPEX.[12]

At every stage after the traveler is referred to secondary inspection, CBP and/or ICE maintain records of the examination, detention, retention, or seizure of a traveler's property, including any electronic devices. Additionally, as travelers enter the port area, they are informed through the posting of signage that all vehicles, other conveyances, persons, baggage, packages, or other containers are subject to detention and search. With the publication of this PIA, CBP will work to amend this signage both to state explicitly that electronic devices are subject to detention and search, and to include a Privacy Act Statement providing notice of DHS's authority to collect information from electronic devices. [See Appendix A for the Privacy Act Statement.]

Search

At primary or secondary inspection, a CBP Officer and/or ICE Special Agent may perform a quick, cursory search of the electronic device in front of the passenger. This may be as simple as turning on the device to establish that it is a working device, rather than a shell for concealed contraband, weapons or explosives. CBP or ICE may direct the traveler to turn on the device to establish that it works, or may take the device from the traveler and perform the task itself. A record of the interaction is entered into TECS.[13] Where information found on the electronic device may be relevant to a traveler's admissibility under the Immigration and Naturalization Act (8 U.S.C. § 1101 *et seq.*), a notation may be made in the appropriate CBP or ICE records systems, such as ENFORCE.[14] Where a traveler makes a request and it is operationally feasible to honor such a request, an examination at secondary inspection may take place in a private area, away from other travelers, including traveling companions. If CBP and ICE are satisfied that no further examination is needed, the electronic device is returned to the traveler

[12] For more information about CBP's random examination program, COMPEX, visit: http://www.cbp.gov/xp/cgov/travel/admissibility/random_exams.xml

[13] *See* U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008, 73 FR 77778; U.S. Immigration and Customs Enforcement External Investigations DHS/ICE-009 December 11, 2008, 73 FR 75452..

[14] *See* Enforcement Operational Immigration Records (ENFORCE/IDENT) DHS/ICE-CBP-CIS-001-03, March 20, 2006 71 FR 13987.

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.[15] CBP or ICE may also examine the information on the electronic device outside of the presence of the traveler.[16] If no further search is needed, and the electronic device is not seized, the device is returned to the traveler. There is no specific receipt given to the traveler if the contents of the device are detained for further review, but the device is returned to the individual. Where CBP performs the search, a supervisor is notified or present for the search.[17]

Detention of Electronic Devices

In most cases, when CBP or ICE keeps the device and the traveler leaves the port without it, the electronic device is considered "detained."[18] For CBP, the detention of devices ordinarily should not exceed five (5) days, unless extenuating circumstances exist.[19] The CBP Officer or ICE Special Agent notes the detention in TECS and provides Customs Form (CF) 6051D to the traveler as a receipt.[20] This form contains contact information for the traveler and the CBP Officer or ICE Special Agent to ensure each party can contact the other with questions or for retrieval of the electronic device at the conclusion of the border search. The CF 6051D is kept with the electronic device and records the chain of custody between the traveler and CBP and/or ICE until final disposition of the case.[21] 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.[22] In such instances, CBP will also provide the traveler with a tear sheet containing information concerning CBP/DHS's authority to perform its search, detention, and possible seizure. [See Appendix B for tear sheet.] The tear sheet further informs the traveler of redress procedures and administrative rights concerning privacy and civil liberties.[23] CBP will work to implement the tear sheet at all ports of entry as expeditiously as possible, but no later than 30 days after the implementation of the new Directive and the issuance of this PIA.

When CBP detains an electronic device under its border search authority, the device may be shared with ICE or another federal agency for analysis.[24] If there is no evidence of criminal activity relating to laws enforced by ICE or CBP, or of a violation of law that subjects the device to seizure for civil forfeiture, the electronic device is returned to the traveler in its original condition, and any copies of the information from the device are destroyed as explained below.[25] If CBP determines the device should be referred to ICE for any reason, or if ICE is the agency of record on the detention, the chain of custody

---

[15] *See* below at "Demands for Assistance" for a discussion of detention of information.
[16] *See* Attachment 1, CBP Directive CD 3340-049, "Border Search of Documents and Electronic Devices Containing Information," August 20, 2009, at 3-4 (hereinafter "CBP Directive"); See Attachment 2, ICE Directive No. 7-6.1, "Border Searches of Documents and Electronic Devices," August 18, 2009, at 3-4 (hereinafter "ICE Directive").
[17] CBP Directive at 3.
[18] Alternatively, the item may be "seized" as evidence of a crime. *See infra* at 10, "Seizure."
[19] CBP Directive at 4.
[20] CBP Directive at 5; ICE Directive at 4-5.
[21] CBP Directive at 5-6.
[22] CBP Directive at 7-8.
[23] CBP Directive at 4-5.
[24] CBP Directive at 5; ICE Directive at 7.
[25] *See infra* at 10, "Destruction."

will reflect that ICE is in possession of the device or information therefrom. Appropriate notations are made in CBP systems of records and on the CF 6051D to reflect the transfer to ICE, and ICE assumes responsibility for the device.

Instead of detaining the electronic device, CBP or ICE may instead copy the contents of the electronic device for a more in-depth border search at a later time. For CBP, the decision to copy data contained on an electronic device requires supervisory approval.[26] Copying may take place where CBP or ICE does not want to alert the traveler that he is under investigation; where facilities, lack of training, or other circumstances prevent CBP or ICE from performing the search at secondary inspection; or where the traveler is unwilling or is unable to assist, or it is not prudent to allow the traveler to assist in the search (such as providing a password to log on to a laptop). If a copy of data on a traveler's electronic device is made on-site and the device is returned to the traveler, a notation of the search is recorded in TECS.[27] The copy is stored on either an ICE external hard drive or computer system, neither of which is connected to a shared or remote network; however, notes from the search may be stored in one of the systems of records listed below (see "SORNs"). For example, information found on the electronic devices that pertains to the traveler's admissibility may be noted in ENFORCE.[28]

In accordance with the Privacy Act, CBP is working to amend signage at ports of entry to state explicitly that electronic devices are subject to detention and search, and to include a Privacy Act Statement providing notice of CBP's and ICE's authority to retain information from electronic devices. CBP will also include this Privacy Act statement on the tear sheet in instances where the individual's electronic device has been detained or seized. [See Appendix B for tear sheet.] CBP will work to implement the tear sheet at all ports of entry as expeditiously as possible, but no later than 30 days after the implementation of the new Directive and the issuance of this PIA.

As federal criminal investigators, ICE Special Agents are empowered to make investigative decisions based on the particular facts and circumstances of each case. The decision to detain or seize electronic devices or detain, seize, or copy information therefrom is a typical decision a Special Agent makes as part of his or her basic law enforcement duties. However, although no additional permission is required at this stage, Special Agents must comply with precise timeframes and supervisory approvals at further stages throughout each border search. The ICE Directive requires that Special Agents complete the border search of any detained electronic device or information in a reasonable time, but typically no longer than 30 days, depending on the facts and circumstances of the particular search.[29] The length of detention depends on several factors, but primarily the amount of information requiring review and the format of that information, which can greatly affect the amount of time necessary to complete a search.[30] If a Special Agent determines there is a need to demand assistance (as described below) for any reason, this time will likely be extended. ICE policy requires that any detention exceeding 30 days, including

[26] CBP Directive at 4.
[27] CBP Directive at 3-4.
[28] *See* Enforcement Operational Immigration Records (ENFORCE/IDENT) DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987.
[29] ICE Directive at 4-5.
[30] ICE Directive at 5.

those where assistance is demanded, must be approved by an ICE supervisor, approved again every 15 days thereafter, and documented in the appropriate ICE record systems.[31]

Demands for Assistance

Where detained information on an electronic device cannot be readily understood, CBP and/or ICE may demand technical assistance, including translation or decryption, from another person or entity without a reasonable articulable suspicion that the data on the electronic device is evidence of a crime.[32] Where CBP or ICE has this reasonable articulable suspicion, CBP and/or ICE may share the information with other federal agencies for subject matter assistance.[33] When CBP demands assistance, CBP informs the assisting party that they must limit the use of the information to the purpose for which it is shared, i.e., decryption, translation, or consistent with providing subject matter assistance. Further, all transmitted information is to be returned to CBP or destroyed with certification provided to CBP within 15 days unless: (1) the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager approves an extension in seven-day increments, or (2) the receiving agency has a valid basis for its own independent authority to seize or continue retention of the transmitted information.[34] If the electronic device is sent to an assisting party, the fact of which is not disclosed to the traveler because of law enforcement or national security concerns, a second chain of custody form (CF 6051D) is created to record the transaction between CBP and the assisting party.[35] This additional CF 6051D is kept with the case file for the electronic device, but is not provided to the traveler because disclosure of transfer to a laboratory or other agency would reveal the existence of a legitimate investigation.[36]

If ICE is unable to complete the search without the assistance of an outside entity, it may demand assistance for translation, decryption, or specific subject matter expertise (e.g., the hard drive failed and ICE requires the assistance of a recovery firm) that may be necessary to allow it to access or understand the detained information.[37] If ICE requires subject matter expertise for information that is not in a foreign language or encrypted, or otherwise requires technical assistance, but nevertheless requires some sort of expertise to assist in review (e.g., scientific materials that require an engineer to review), ICE policy requires that the Special Agent have a reasonable suspicion of activities in violation of the laws enforced by ICE before a demand for assistance may issue.[38] In all instances, ICE policy requires that assistance be demanded in writing, include sufficient details so the assisting agency/entity knows what to look for, and establish timeframes for the responses required by ICE.[39] Demands to assisting federal agencies also include the requirement to return or destroy the information after assistance has been rendered unless the agency possesses independent legal authority to retain such information.[40] Demands to non-federal

[31] ICE Directive at 5.
[32] *See* 19 U.S.C. § 507; CBP Directive at 5-6.
[33] CBP Directive at 5.
[34] CBP Directive at 6-8.
[35] CBP Directive at 6.
[36] CBP Directive at 6.
[37] ICE Directive at 5-6.
[38] ICE Directive at 6.
[39] ICE Directive at 6-7.
[40] ICE Directive at 8.

entities require all information be returned to ICE upon completion of assistance.[41] The Special Agent is required to contact the assisting agency or entity within the first 30 days to get a status report and to continue contact thereafter until a final response is received.[42]

Seizure

When either CBP or ICE determines probable cause exists to seize the electronic device, the seizing Officer or Special Agent completes a chain of custody form (CF 6051S) to reflect the seizure.[43] A seizure record is also made in the Seized Asset and Case Tracking System (SEACATS) and noted in TECS.[44] If the original device is seized in the presence of the traveler, the traveler is given a copy of the CF 6051S at the time of seizure.[45] If the original device has been detained and referred to ICE, and should ICE find probable cause to seize the device, the chain of custody form for the detention (CF 6051D) is superseded by a seizure form (CF 6051S). The seizure form is mailed to the traveler in accordance with applicable laws and regulations for customs seizures.[46] Any CBP records and notes are turned over to ICE for investigation and prosecution. If CBP or ICE did not detain the original device, but instead detained a copy of the data contained on the device, the first copy made is known as the "gold copy"; the chain of custody form stays with the gold copy.

Destruction

Electronic devices are never destroyed unless they are seized for civil forfeiture or as evidence of criminal activity, and are subsequently forfeited to the Government. Electronic devices that are not seized are returned to the traveler as expeditiously as possible following the conclusion of the border search.[47] Copies of information from electronic devices are not retained by CBP or ICE unless retention is required for a law enforcement purpose and is consistent with the system of records that covers the detained information.[48] Detained electronic information that is destroyed is not merely deleted, but forensically wiped, which entails writing over the information multiple times to ensure it cannot be accessed again.[49] Once the electronic copy is forensically wiped, a record of the destruction is documented in the TECS Report of Investigation (ROI), as appropriate.[50]

As stated above under "Detention," CBP or ICE may detain an electronic device or a copy of information on a device in order to determine if it has investigative or enforcement value. Should CBP or ICE determine there is no value to the information copied from the device, that information is destroyed as expeditiously as possible. For CBP and ICE, the destruction must take place no later than seven

---

[41] ICE Directive at 8.
[42] ICE Directive at 7.
[43] ICE Directive at 4.
[44] *See* Seized Assets and Case Tracking System DHS/CBP-013 December 19, 2008, 73 FR 77764.
[45] ICE Directive at 4.
[46] *See* 19 C.F.R. Part 162.
[47] CBP Directive at 4.
[48] This means that if CBP retains the information, CBP retention policy for a particular system of records would govern. If ICE ultimately retains the information, ICE retention policy for a particular system of records would govern.
[49] CBP Directive at 2.
[50] CBP Directive at 4; ICE Directive at 8.

calendar days after such determination[51] unless circumstances require additional time. If additional time is required, the supervisor must approve and document it in the appropriate CBP or ICE system of records. Under no circumstance will the destruction be later than 21 calendar days after the determination that there is no value to the information.[52] If CBP or ICE determines the information should be retained because the information is required for law enforcement purposes and is relevant to immigration, customs, or other laws enforced by DHS, the information and the record of the retention are recorded in a DHS system of records.[53]

Safeguards of Information by CBP

In addition to the record-keeping requirements explained above, including the chain of custody protocols and the systems of records notices, CBP has further oversight and auditing procedures to ensure the proper management and security of information retained for electronic devices or information detained or seized.

While CBP Officers are responsible for the examination of electronic devices, only Supervisors may authorize the copying of the contents of an electronic device.[54] Where an electronic device is to be detained or seized by CBP, a CBP Supervisor must approve of the detention or seizure, and the CBP Officer must provide a completed CF 6051D or S, respectively, to the traveler.[55] Where a traveler claims that the contents of the electronic device contain attorney-client or other privileged material, the CBP Officer must consult with the local Associate/Assistant Chief Counsel or United States Attorney's Office before conducting the examination.[56]

CBP Supervisors may authorize the sharing of the traveler's information for assistance or other law enforcement purpose on a case-by-case basis. Materials must be returned within 15 days, unless the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager approves an extension in seven-day increments, as described above.[57]

With regard to oversight of the seizure policy, the Commissioner of CBP is the ultimate authority concerning any seizures and forms issued to the parties involved. CBP Port Directors are required to develop, implement, and update any necessary additional port-specific procedures to ensure the proper accountability of the property examined, detained, or seized and proper forms are utilized. The Duty Supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished. The appropriate CBP Second Line Supervisor shall approve and monitor the status of the detention of all documents or electronic devices or copies of information contained therein. The appropriate CBP Second Line Supervisor shall approve and monitor the status of the transfer of any document or electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another federal agency.[58] The Seized

[51] CBP Directive at 4.
[52] ICE Directive at 8.
[53] CBP Directive at 7; ICE Directive at 7.
[54] CBP Directive at 4.
[55] CBP Directive at 5.
[56] CBP Directive at 3-4.
[57] CBP Directive at 6.
[58] CBP Directive at 9.

Property Custodians/Specialists (SPC/SPS) must ensure preservation, safeguarding, and disposition of all property/evidence released to their custody.

Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during transmission such as password protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized must be immediately reported to the Port Director, Patrol Agent in Charge or equivalent level manager and the CBP Office of Internal Affairs.[59]

Safeguards of Information by ICE

ICE handles border searches of electronic devices with the same caution and care afforded during searches of any other personal belongings, including paper documents. In this regard, ICE does not distinguish between the search of electronic devices and a diary, briefcase, or suitcase; ICE Special Agents are required to protect all personal items, information, and any sensitive information contained therein in the same manner.

ICE has various safeguards in place to protect electronic devices that are detained or seized, or information from a device that is detained during a border search.[60] ICE stores all electronic devices, or information thereof, in locked cabinets and rooms and maintains a chain of custody using appropriate ICE forms and systems.[61] If a copy of information is made from the electronic device to allow the traveler to leave the port of entry with his device, the first copy is known as the "gold copy." The chain of custody stays with the original or gold copy so that it may be used as evidence in court, if necessary. A new chain of custody form is issued to follow any additional copy of the data that is made; such forms are tracked by ICE Special Agents in the appropriate ICE systems.

By policy, ICE's review of detained information is to be completed in a reasonable time and, if the original device has been detained by ICE, the ICE Special Agent must provide a chain of custody form to the traveler as a receipt.[62] Special Agents must factor in the time necessary for any assistance that may be required when determining "reasonable time."[63] Once the border search is completed, the detained device will either be seized or returned to the traveler and any copy of the data from the device will be retained for law enforcement purposes and in accordance with the established retention periods for any system of records in which it is stored or destroyed.[64]

As described above, all Special Agents perform border searches on electronic devices; however, only those trained by ICE and certified as CFAs are permitted to extract information from electronic devices for evidentiary purposes. CFAs are specially trained on information technology, evidentiary, and legal issues involving the search, analysis, duplication, and seizure of electronic information. Within ICE, only CFAs are permitted to make copies of data stored on electronic devices during a search to ensure secure and accurate duplication of the information, and the integrity of the information (original

[59] CBP Directive at 8.
[60] ICE Directive at 7.
[61] ICE Directive at 7.
[62] ICE Directive at 4.
[63] ICE Directive at 5.
[64] ICE Directive at 7.

and copy) and the electronic devices. (Unless otherwise specified, any reference to ICE Special Agents in this PIA also includes CFAs.) CFAs are also trained in the proper and secure destruction of electronic information.

ICE policies and procedures that safeguard this information are enforced through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files, documentation required for forensic examinations, and random and routine inspections of field offices. Inspections delve into every aspect of the ICE Special Agent's responsibilities, ranging from security of the hardware and facility, to training and recordkeeping. All ICE Special Agents are required to take yearly training courses, available through the ICE Virtual University, including annual Information Assurance Awareness Training, which stresses the importance of good security and privacy practices, and Records Management Training, which stresses agency and individual responsibilities related to record creation, maintenance, use, retention and disposition. Additionally, in the coming months, ICE Special Agents will be required to complete a new training course specifically focusing on ICE's Directive on border searches of electronic devices. This training will focus on ICE policies with respect to searches involving sensitive information (e.g., privileged material) and other procedural requirements and safeguards. The training is intended to reinforce Special Agents' knowledge of the ICE policy and to serve as a reminder to treat such searches with special care. Additionally, CFAs are required to take annual continuing education classes specific to computer and digital forensics, which may include the latest techniques and methods on copying, analyzing, and destroying electronic information.

ICE recognizes electronic devices have the capacity to store sensitive information, however a traveler's claim of privilege or statement to an ICE Special Agent that something is personal or business-related does not preclude the search.[65] ICE policy and certain laws, such as the Privacy Act and the Trade Secrets Act, requires the special handling of some types of sensitive information including attorney-client privileged information, proprietary business information, and medical information.[66] Special Agents violating these laws and policies are subject to administrative discipline and criminal prosecution. Further, when a Special Agent suspects that the content of electronic devices includes attorney-client privileged material that may be relevant to the laws enforced by ICE, ICE policy requires the Special Agents to contact the local ICE Chief Counsel's office or the local U.S. Attorney's Office before continuing a search.[67]

During transmission to other federal agencies and non-federal entities for assistance, ICE takes appropriate measures to safeguard the information, to include, encrypting electronic information where appropriate, storing in locked containers, and hand delivery. In addition to the demand letter that is sent to assisting agencies and entities, the information and devices sent for analysis is accompanied by a chain of custody form.

When ICE determines that electronic devices or information may not be kept by ICE pursuant to its Directive, any copies of information obtained from such devices are destroyed.[68] The destruction technique follows ICE policies with regard to the particular form of information, is coordinated with the

[65] ICE Directive at 9.
[66] ICE Directive at 9.
[67] ICE Directive at 9.
[68] ICE Directive at 8.

United States Attorney's Office in the case of a federal prosecution, is recorded appropriately in ICE systems, and requires approval by a Supervisor. The original device, if it has been detained, is returned to the traveler as expeditiously as possible.[69]

In the event that electronic device or information that has been detained, retained, or seized by ICE is known or suspected to be lost or compromised, the incident is reported immediately to the ICE Computer Security Incident Response Center. The loss or compromise of personal information will be handled pursuant to the DHS Privacy Incident Handling Guide.[70]

Summary of Privacy Risks

This PIA analyzes how CBP and ICE will handle the examination, detention, retention, and seizure of electronic devices and information.[71]

CBP and ICE have identified six privacy risks associated with the examination, detention, retention, and/or seizure of a traveler's electronic device or information during a border search: (1) travelers may need additional information regarding the authority to conduct border searches; (2) the traveler may be unaware of the viewing or detention of his/her information by CBP and ICE; (3) personally identifiable information (PII) may be detained where it is not needed; (4) PII may be misused by CBP and ICE officers; (5) CBP and ICE may disclose PII to other agencies that may misuse or mishandle it; and (6) new privacy risks may arise as the technology involved in this activity is ever-changing. The first risk is disposed of by the overwhelming precedent in U.S. law which affords CBP and ICE latitude in conducing searches of individuals and their belongings as they cross the United States borders. Particular means of mitigating risks two through five are discussed below. The sixth risk is further mitigated through the ongoing involvement of the DHS Privacy Office, and the commitment of CBP and ICE to revise and re-issue the applicable CBP and ICE directives, as well as this PIA when necessary.

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. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer of DHS 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 DHS's information collection.

---

[69] ICE Directive at 4; see also *supra* at 10, Destruction.
[70] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[71] This assessment does not evaluate the activities of other Federal, State, and local agencies. The Privacy Office will work with CBP and ICE to evaluate any policies and procedures which may be proposed in the future and update this PIA as necessary.

DHS conducts PIAs on Department practices and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. The search, detention, seizure, and retention of electronic devices through a border search is a DHS practice; as such, this PIA is conducted 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.*

When ICE or CBP retain information from electronic devices, that information may be subject to the requirements of the Privacy Act. The Privacy Act requires that agencies publish a System of Records Notice (SORN) in the *Federal Register* describing the nature, purpose, maintenance, use, and sharing of the information. This PIA and the several SORNs published by DHS provide notice of the retention of PII at the border and the retention of some of the contents of electronic devices.

CBP has two principal SORNs that provide notice regarding the border search and seizure of electronic devices. First, the TECS SORN,[72] which covers, among other things, any records of any inspections conducted at the border by CBP, including inspections of electronic devices. Second, CBP's SEACATS SORN provides notice regarding any seizures, fines, penalties, or forfeitures associated with the seizure of electronic devices.[73] ICE has several SORNs that provide notice regarding the border search, detention, seizure, and retention of electronic devices and information. The ICE Search, Arrest, and Seizure Records SORN,[74] covers the information detained and seized by ICE as described in this PIA, specifically "seized or detained records in both paper and electronic form, including computers, computer records, disks, hard drives, flash drives, and other electronic devices and storage devices."[75] ICE may also maintain the information described in this PIA in one or more recordkeeping systems covered by the Alien File and Central Index System SORN[76] and the following ICE SORNs: ENFORCE/IDENT SORN;[77] ICE Pattern Analysis and Information Collection (ICEPIC) SORN;[78] and External Investigations SORN.[79]

These SORNs provide overall notice and descriptions of how CBP and ICE function 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

[72] *See* U.S. Customs and Border Protection TECS DHS/CBP-011 December 19, 2008, 73 FR 77778.
[73] *See* Seized Assets and Case Tracking System DHS/CBP-013 December 19, 2008, 73 FR 77764.
[74] Search, Arrest, and Seizure Records DHS/ICE-008, December 9, 2008, 73 FR 74732.
[75] *See* Search, Arrest, and Seizure Records DHS/ICE-008, December 9, 2008, 73 FR 74732.
[76] *See* Alien File (A-File) and Central Index System (CIS) DHS-USCIS-001, January 16, 2007, 72 FR 1755.
[77] *See* Enforcement Operational Immigration Records (ENFORCE/IDENT) DHS/ICE-CBP-CIS-001-03, March 20, 2006, 71 FR 13987.
[78] *See* ICE Pattern and Analysis and Information Collection (ICEPIC) DHS/ICE-002, August 18, 2008, 73 FR 48226.
[79] *See* External Investigations DHS/ICE-009, December 11, 2008, 73 FR 75452.

information that is retained from an electronic device and maintained in a CBP or ICE system of records will be secured and protected in the same manner as all other information in that system.

CBP Policy Transparency

To provide additional transparency to the public regarding CBP border search policy, signage is posted notifying travelers that all vehicles, other conveyances, persons, baggage, packages, or other containers are subject to detention and search. With the publication of this Privacy Impact Assessment, CBP will work to amend this signage both to state explicitly that electronic devices are subject to detention and search, and to include a Privacy Act Statement providing notice of DHS's authority to collect information from electronic devices. [See Appendix A for Privacy Act Statement.] Further, CBP is publishing CBP Directive CD 3340-049, "Border Search of Documents and Electronic Devices Containing Information" (August 20, 2009) in tandem with this PIA. [See Attachment 1 for CBP's Directive and Attachment 2 for ICE's Directive] Previously, CBP also made public a policy memorandum of July 16, 2008 entitled "Policy Regarding Border Search of Information."[80] CBP has also posted information on its website regarding the issue of laptop examinations and random searches.[81] Lastly, when CBP detains or seizes an electronic device the traveler will be provided with a tear sheet, which informs her or him of the Authority for CBP/DHS's action, and provides notice as to the procedures the traveler may follow for seeking redress.[82] While generally informative, these publications do not describe all aspects of the examination and detention of electronic devices because providing specific transparency to the general public about all aspects of the program could compromise law enforcement or national security sensitive information. CBP will work to implement the tear sheet at all Ports of Entry as expeditiously as possible, but no later than 30 days after the implementation of the new Directive and the issuance of this PIA.

ICE Policy Transparency

ICE's conduct of border searches of electronic devices is governed by directive.[83] Safeguards included in the ICE directive are described throughout this PIA. ICE is publishing ICE Directive 7-6.1, "Border Searches of Documents and Electronic Devices" as an Attachment to this PIA. [See Attachment 2 for ICE Directive]. If the ICE policy is modified, ICE will update this PIA to ensure the public's understanding remains current about the nature and extent of these searches, as well as the controls and safeguards that exist to protect the individual's rights and the information being searched. At a minimum, this PIA broadens the public's understanding of ICE's role in border searches of electronic devices.

Information Sharing Transparency

Because notifying the traveler of the sharing of information could impede an investigation or other law enforcement or national security efforts, CBP and ICE do not make the information sharing process fully transparent to the public. To ensure the protection of personal data without compromising

[80] Available at: http://www.cbp.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf.
[81] Available at: http://www.cbp.gov/xp/cgov/travel/admissibility/authority_to_search.xml, http://www.cbp.gov/xp/cgov/travel/admissibility/labtop_inspect.xml, and http://www.cbp.gov/xp/cgov/travel/admissibility/random_exams.xml.
[82] *See* Appendix B, "Customer Service Contacts" p. 2.
[83] ICE Directive at 3.

the investigation, CBP and ICE have instituted strict oversight and review processes. Generally speaking, information, including PII, will be shared with other agencies where CBP and/or ICE require subject matter expertise, decryption, or translation. Where PII is disseminated to other agencies, CBP and ICE will ensure the sharing is permissible under the Privacy Act of 1974, including whether (1) the requesting agency has an official need to know the information and (2) an appropriate routine use exists under the relevant SORN.

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.*

Individual participation provides complementary benefits for the public and the government. The government is able to maintain the most accurate information about the public, and the public is given greater access to the amount and uses of the information maintained by the government. A traditional approach to individual participation is not always practical for agencies like CBP and ICE which have law enforcement and national security missions. The U.S. Supreme Court has recognized that presenting one's self at the U.S. border seeking to enter has been equated with consent to be searched.[84] 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 U.S. government's ability to protect its borders and diminish the effectiveness of such searches, thereby lessening our overall national security. 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. CBP and ICE will involve the individual in the process to the extent practical given the facts and circumstances of the particular border search.[85] Should the border search continue away from the traveler, the traveler will be notified if his or her electronic device is detained or seized.[86] In instances when direct individual participation is inappropriate, well-documented processes, well-trained CBP Officers and ICE Special Agents, 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 purpose specification principle requires DHS to 1) articulate the authority to retain the PII in question, as well as 2) articulate the purpose(s) for which DHS will use the PII.

---

[84] *See, e.g., U.S. v. Flores-Montano*, 541 U.S. 149 (2004), *U.S. v. Ramsey*, 431 U.S. 606 (1977).
[85] CBP Directive at 3; ICE Directive at 3-4.
[86] CBP Directive at 4-5; ICE Directive at 4.

Information is authorized to be detained, retained, or seized and subsequently used by CBP or ICE to carry out their law enforcement missions under numerous authorities, including: 19 U.S.C. § 482 (Search of vehicles and persons), 19 U.S.C. § 1461 (Inspection of merchandise and baggage); 19 U.S.C. § 1496 (Examination of baggage); 19 U.S.C. § 1499 (Examination of merchandise); 19 U.S.C. § 1582 (Search of persons and baggage); 19 C.F.R. Part 162 (Inspection, Search, and Seizure); 8 U.S.C. § 1225 (Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing); and 8 U.S.C. § 1357 (Powers of immigration officers and employees).

The authority for border searches is well-established in law.[87] Allowing the traveler to dictate the extent of a border search, the detention and seizure of an electronic device, or retention and sharing of the information encountered during that search would interfere with U.S. government's ability to protect its borders and diminish the effectiveness of such searches, thereby lessening our overall national security.

Because CBP and ICE enforce 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 provide evidence of violations of law, including importing obscene material, drug smuggling, other customs violations, or terrorism, among others.[88] The information will be used by ICE to conduct investigations into criminal and civil violations of laws, and to carry out the immigration laws of the United States. 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. Consistent with applicable laws and SORNs, information lawfully seized by CBP and ICE may be shared with other state, local, federal, and foreign law enforcement agencies in furtherance of enforcement of their laws.

4. Principle of 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).*

All CBP and ICE policies and procedures relating to border search of electronic devices seek to minimize the retention of information to that which is relevant and necessary to carry out the law enforcement purpose of the search. When CBP or ICE detain electronic devices for a border search, each agency has established timeframes so as to limit the amount of time PII is detained (unless ultimately seized) as much as possible. A detained device that is not seized is returned to the traveler as expeditiously as possible and is logged in TECS. For CBP, the detention of devices ordinarily should not exceed five (5) days, unless extenuating circumstances exist.[89] The Port Director, Patrol Agent in Charge, or other equivalent level manager approval is required to extend any such detention beyond five (5) days.[90] When CBP detains, seizes, or retains electronic devices, or copies of information therefrom,

[87] *See U.S. v. Flores-Montano*, 541 U.S. 149 (2004); *U.S. v. Ramsey*, 431 U.S. 606 (1977).
[88] A more complete summary of statutes enforced by CBP is available at: http://www.cbp.gov/linkhandler/cgov/trade/legal/summary_laws_enforced/summary_laws.ctt/summary_laws.doc.
[89] CBP Directive at 4.
[90] CBP Directive at 4.

and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.[91]

By policy, ICE may only detain the device or information for a reasonable time, which is dependent on the facts and circumstances of the particular search, but is typically no more than 30 days.[92] Detentions may not exceed 30 days unless approved by an ICE supervisor, and approved again every 15 days thereafter.[93] Any such approvals will be documented in appropriate ICE records systems.[94] Any information copied in this process, once it is determined to be of no value, will be destroyed within seven days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate records systems, but no later than 21 calendar days after such determination.[95]

In addition, at any point during a border search, the CBP Officer or ICE Special Agent may make a determination to seize the electronic device (for criminal law enforcement purposes) or retain information (for immigration, customs, or other law enforcement purposes). An electronic device that has been seized is considered evidence and is maintained in accordance with applicable ICE and CBP policies and procedures.[96] Generally, seized evidence is retained until final disposition through judicial adjudication or criminal, civil, or administrative forfeiture actions. In the case of a judicial proceeding, destruction of the evidence, if appropriate, is permitted after all appeals have been exhausted or when a plea agreement includes forfeiture. Retained information is maintained for a period concurrent with the DHS systems in which such information is included.

When demanding assistance for translation, decryption, or subject matter expertise, CBP and ICE require the demand be made in writing (i.e., a demand letter or, in a taskforce scenario, documentation of the demand and circumstances in appropriate systems) with sufficient details of the matter at hand and the particular request so that the assisting agency or entity knows what to look for, is aware of the timeframes set by CBP or ICE, and the responses required by CBP or ICE.[97] Whenever practicable, CBP and ICE share only the portion of the information for which assistance is required to minimize unnecessary sharing of information. Demands to assisting federal agencies advise of the requirement to return or destroy the information after assistance has been rendered unless it possesses independent legal authority to retain such information.[98] Demands to non-federal entities require all information be returned to ICE upon completion of assistance.[99] Ultimately, the responsibility to act in accordance with the CBP or ICE directives lies with the Officer or Special Agent demanding assistance.[100]

---

[91] CBP Directive at 2.
[92] ICE Directive at 4-5.
[93] ICE Directive at 4-5.
[94] ICE Directive at 4-5.
[95] ICE Directive at 8.
[96] CBP Directive at 7-8; ICE Directive at 7-8.
[97] CBP Directive at 5-8; ICE Directive at 6.
[98] CBP Directive at 7-8; ICE Directive at 8.
[99] ICE Directive at 8.
[100] CBP Directive at 8-9; ICE Directive at 3-5.

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.*

CBP and ICE Sharing of Detained Information

As a matter of policy, CBP and ICE only copy and detain a traveler's information pursuant to the border search authority to resolve immigration, customs, and/or other law enforcement matters. Where information is shared with an agency outside of CBP, ICE, or DHS for assistance (such as translation, decryption, or subject matter expertise), the receiving agency is informed that they must limit the use of the information to the purpose of the sharing and return or destroy all information after analysis unless they have separate statutory authority to retain it.[101] Once the matter has been resolved, such information is returned or destroyed, as described above.[102]

With regard to an electronic device that has merely been detained before a conclusion to the border search has been made, in limited circumstances ICE or CBP may be required to share certain information with other federal agencies pursuant to appropriate Presidential Directives and Executive Orders.

CBP and ICE Sharing of Seized and/or Retained Information

As federal law enforcement agencies, CBP and ICE have 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.[103] To ensure that a traveler's seized and/or retained information is used for the proper purpose, all CBP and ICE 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 or ICE systems and/or is recorded by those systems' audit functions.

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.*

CBP Data Quality and Integrity

CBP anticipates routinely detaining PII in the course of the examination and detention of electronic devices. Because CBP accesses electronic devices for purposes of law enforcement,

[101] CBP Directive at 6-8; ICE Directive at 6, 8-9.
[102] CBP Directive at 8; ICE Directive at 8.
[103] *See, e.g.,* 19 U.S.C. § 1628.

discrepancies between the information possessed by the traveler and information detained by CBP may present privacy risks. Inaccurate, irrelevant, untimely, or incomplete information may result in cases moving to prosecution where none is warranted, or may result in cases being dismissed where a violation has occurred.

To ensure the PII is accurately recorded, CBP takes forensic 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 or investigation has reached a conclusion, at which time copies of the information are destroyed, unless further retention is appropriate and consistent with the appropriate retention schedule.[104] Information entered into TECS, SEACATS, and other systems of records are kept with annotations noting the time they were added to the file for contextual relevancy.

ICE Data Quality and Integrity

As explained in Section 4 above (Minimization), ICE's policies and procedures are targeted toward limiting the amount of information that is held by ICE to that which is relevant and necessary for a law enforcement purpose, such as a criminal or civil investigation, or the admissibility of an alien into the United States. Information that is retained or seized by ICE during a border search is actual or potential evidence that may be used in a criminal, civil, or administrative proceeding. Therefore, ICE cannot alter the information to correct any inaccuracies without seriously compromising the integrity of the investigation and potentially violating federal evidentiary rules and rules of civil and criminal procedure.

To the extent that information that is retained may be inaccurate, untimely, or incomplete, the investigatory process is intended to identify evidence and other information that may be flawed or conflict with other information that is retained during the investigation. If the information is used as evidence in a civil or criminal prosecution, or if an individual is in immigration proceedings, rules of evidence and procedure and constitutional protections entitle the individual to certain due process protections with respect to the use of the information against him, including the ability to challenge the authenticity of the information and to call witnesses to dispute the quality or integrity of the information. These protections provide an adequate safeguard against inaccurate, incomplete, or out-of-date information that may be included in the information.

With respect to information integrity and quality issues in the context of the retention, duplication, and analysis of the information, ICE uses the most current technology available and places great importance on training its CFAs in the latest techniques to preserve the quality and integrity of information subject to search. To ensure the information is accurately recorded, ICE takes precautions to prevent the alteration of the information on the electronic device and, if a copy is made, on the copy as well. The information is always handled with concern for its ultimate potential use as evidence in court; as such, ICE Special Agents are very careful to preserve the quality and integrity of the information to avoid damaging their investigation. Any inaccurate information is the result of the traveler having inaccurate information on his or her electronic devices, rather than errors in the copying by the CFA. To ensure the information is relevant, if no relevant information is found, ICE only retains the information

[104] CBP Directive at 7-8; ICE Directive at 7-8.

until the border search has reached a conclusion, at which time any originals are returned to the traveler and all copies are destroyed.[105]

Information being brought across the borders is subject to search, detention, retention, and seizure, regardless of the true owner of the information. However, ICE recognizes that persons in possession of electronic devices may not always have complete control or ownership over the information contained therein. In such cases, ICE establishes knowledge and ownership of such information through a variety of means, including interviews, further investigation, and a forensic review of the devices.

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.*

Because the examination of an electronic device takes place in the context of a traditional border search, CBP and ICE have many existing procedures in place to safeguard data. For example, CBP and ICE personnel must comply with the Privacy Act, the Trade Secrets Act, and the Federal Information Security Management Act (FISMA) and other statutes, Executive Orders, and regulations in the collection, storage, use, protection, and disclosure of information collected, retained, or seized during a border search. The protective strategies for this information are physical, technical, and administrative in nature, and provide access control to sensitive information, physical access control to DHS facilities, confidentiality of communications, and personnel screening.[106]

During an examination at secondary inspection, CBP Officers and ICE Special Agents are trained to inspect the electronic device in such a way to prevent other travelers, including traveling companions, from viewing the contents of the electronic device. Further, the examination may be carried out in a separate area away from other travelers, if the traveler requests it and facilities are available. More in-depth searches of electronic devices are conducted in secure locations with restricted access. Detained and seized devices are always securely maintained in a CBP or ICE facility with access limited to only authorized personnel or authorized and escorted visitors. Physical security includes security guards and locked facilities requiring badges and passwords for access. To address the risk of a physical security intrusion, electronic devices will be stored in vaults, safes or locked cabinets accessible only to authorized government personnel and contractors who are properly screened, cleared, and trained in information security and the protection of privacy information.[107]

All CBP and ICE personnel with access to detained and seized electronic devices and information are screened through background investigations commensurate with the level of access required to perform their duties. Only ICE personnel (CFAs) who are authorized to perform the search and analysis of electronic devices have access to the computer systems containing this information, which are typically stand-alone systems or limited-access local area networks. IT system safeguards prevent unauthorized access, monitor use, and record all actions taken with respect to a traveler's electronic information.

---

[105] ICE Directive at 4, 8.
[106] CBP Directive at 7-8; ICE Directive at 7-9.
[107] CBP Directive at 7-8; ICE Directive at 7.

Electronic devices and information will be maintained in and only accessible from secured systems through hardware and software devices protected by appropriate physical and technological safeguards, including password protection to prevent unauthorized access.

Finally, CBP and ICE policies and procedures that safeguard this information are enforced through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files, documentation required for forensic examinations conducted by ICE CFAs, and periodically administering audits.[108] Recognizing the inherent law enforcement aspect of these searches, to mitigate the privacy risk of obtaining and storing the information that is contained in a traveler's electronic device without the traveler's direct knowledge, CBP and ICE have strict recordkeeping, auditing, and oversight requirements. These measures provide specific guidance about obtaining and storing of the contents of a traveler's electronic device to those who implement and oversee the program both inside and outside DHS. Clear policies and procedures, in conjunction with regular reporting, reviews, and audits, ensure that personal information is effectively protected without negatively impacting the effectiveness of CBP and ICE law enforcement activities.

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.*

CBP Accountability and Auditing

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.

Records of the examination, copying, maintenance, and sharing of the information are maintained to provide constant oversight. Examinations and detentions are recorded in TECS by the CBP Officer or ICE Special Agent.[109] When an electronic device is seized, a record is kept in SEACATS. When CBP or ICE shares the information with an agency outside of DHS, a CF 6051D or S form is created to log the chain of custody. Finally, CBP Management Inspection conducts periodic audits of all systems in order to ensure that the border searches are conducted in accordance with CBP policies.[110]

[108] CBP Directive at 8-9.
[109] CBP and ICE each use the TECS system and may create and edit entries.
[110] CBP Directive at 9.

Effective oversight and recordkeeping provide the means for verifiable accountability and the ability to be audited. CBP conducts regular self-assessments to verify compliance with its responsibilities. The DHS Privacy Office will also provide ongoing guidance on all privacy issues raised by significant or novel legal questions. Finally, the DHS Privacy Office will be part of the process to make improvements as technology changes to make sure that all future technology is implemented consistent with all privacy policies, procedures and applicable privacy laws. As the methods and policies of examining and detaining electronic devices evolve, this PIA will be updated, as appropriate.

ICE Accountability and Auditing

ICE is held accountable for complying with these principles and its border search of documents and electronic devices directive through a variety of oversight mechanisms, including requirements to appropriately document these activities in case files, documentation required for forensic examinations, and random and routine inspections of field offices. Inspections delve in to every aspect of the ICE Special Agent's responsibilities, ranging from security of the hardware and facility, to training and recordkeeping. All ICE Special Agents are required to take yearly training courses including annual Information Assurance Awareness Training, which stresses the importance of good security and privacy practices, and Records Management Training which stresses agency and individual responsibilities related to record creations, records maintenance and use, and retention and disposition of records. Additionally, in the coming months, ICE Special Agents will be required to complete a new training course specifically focusing on ICE's Directive on border searches of electronic devices. This training will focus on ICE policies with respect to searches involving sensitive information (e.g., privileged material) and other procedural requirements and safeguards. The training is intended to reinforce Special Agents' knowledge of the ICE Directive and to serve as a reminder to treat such searches with special care.

Effective oversight and recordkeeping provide the means for verifiable accountability and ability to be audited. ICE conducts regular self-assessments to verify compliance with its responsibilities. In addition, detentions exceeding 30 days must be approved by an ICE supervisor.[111] The DHS and ICE Privacy Offices will also provide ongoing guidance on all privacy issues raised by significant or novel legal questions. Finally, the DHS and ICE Privacy Offices will participate in future decisions regarding technology advances in search techniques to ensure implementation is consistent with all the Fair Information Practice Principles, as well as privacy policies, procedures and laws. As the methods and policies of examining and detaining electronic devices evolve, this PIA will be updated, as appropriate.

Responsible Officials

Laurence Castelli
Chief, Privacy Act Policy and Procedures Branch, Regulations & Rulings
Office of International Trade
U.S. Customs and Border Protection, Department of Homeland Security

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

[111] ICE Directive at 10.

Appendix A

Privacy Act Statement

Pursuant to 5 U.S.C. § 552a (e)(3), this Privacy Act Statement serves to inform you of the following concerning the possible collection of information from your electronic device.

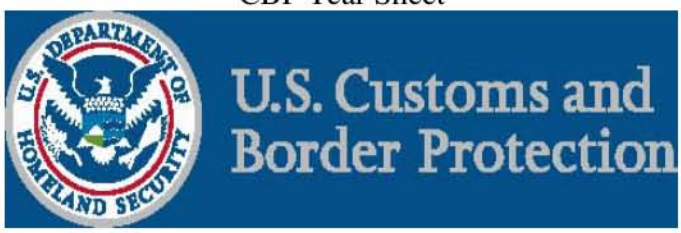
AUTHORITY and PURPOSE: All persons, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search and detention. This is because CBP must determine the identity and citizenship of all persons seeking entry into the United States, determine the admissibility of foreign nationals, and deter the entry of possible terrorists, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items. CBP are charged with enforcing various laws that authorize such searches and detention (see, for example, 8 U.S.C. §§ 1225 and 1357, 19 U.S.C. §§ 482, 507, 1461, 1496, 1499, 1581, 1582, and 1595a(d), 22 U.S.C. § 401, and 31 U.S.C. § 5317, as well as the attending regulations of U.S. Customs and Border Protection promulgated at Titles 8 and 19 of the Code of Federal Regulations).

ROUTINE USES: The subject information may be made available to other agencies for investigation and/or for obtaining assistance relating to jurisdictional or subject matter expertise, or for translation, decryption, or other technical assistance. This information may also be made available to assist in border security and intelligence activities, domestic law enforcement and the enforcement of other crimes of a transnational nature and shared with elements of the federal government responsible for analyzing terrorist threat information.

CONSEQUENCES OF FAILURE TO PROVIDE INFORMATION: Collection of this information is mandatory at the time that CBP seeks to copy information from the electronic device. Failure to provide information to assist CBP in the copying of information from the electronic device may result in the detention and/or seizure of the device.

Appendix B

CBP Tear Sheet



Electronic Devices

Why You May Be Chosen for An Inspection

You may be subject to an inspection for a variety of reasons, some of which include: your travel documents are incomplete or you do not have the proper documents or visa; you have previously violated one of the laws CBP enforces; you have a name that matches a person of interest in one of the government's enforcement databases; or you have been selected for a random search. If you are subject to inspection, you should expect to be treated in a **courteous, dignified, and professional** manner. If you have questions or concerns, you may ask to speak with a CBP supervisor.

Purpose for and Authority to Search

All persons, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search and detention. This is because CBP officers must determine the identity and citizenship of all persons seeking entry into the United States, determine the admissibility of foreign nationals, and deter the entry of possible terrorists, terrorist weapons, controlled substances, and a wide variety of other prohibited and restricted items. CBP is charged with enforcing various laws that authorize such searches and detention (see, for example, 8 U.S.C. §§ 1225 and 1357, 19 U.S.C. §§ 482, 507, 1461, 1496, 1499, 1581, 1582, and 1595a(d), 22 U.S.C. § 401, and 31 U.S.C. § 5317, as well as the attending regulations of U.S. Customs and Border Protection promulgated at Titles 8 and 19 of the Code of Federal Regulations).

What Happens Now?

You are receiving this sheet because your electronic device(s) has been detained for further examination, which may include copying. The **CBP officer** who approved the detention will speak with you and explain the process. You will receive a written receipt (Form 6051-D) that details what item(s) is being detained, who at CBP will be your point of contact, and your contact information (including telephone number) to facilitate the return of your property within a reasonable time upon completion of the examination. Some airport locations have dedicated **Passenger Service Managers** who are available in addition to the onsite supervisor to address any concerns.

Return or Seizure of Detained Electronic Devices(s)

CBP will contact you by telephone when the examination of the electronic device(s) is complete, to notify you that you may pick-up the item(s) during regular business hours from the location where the item(s) was detained. If it is impractical for you to pick up the device, CBP can make arrangements to ship the device to you at our expense. CBP may retain documents or information relating to immigration, customs, and other enforcement matters only if such retention is consistent with the privacy and data protection standards of the system in which such information is retained. Otherwise, if there is no probable cause to seize information after review, CBP will not retain any copies.

If CBP determines that the device is subject to seizure under law – for example, if the device contains

evidence of a crime, contraband or other prohibited or restricted items or information – then you will be notified of the seizure as well as your options to contest it through the local CBP Fines, Penalties, and Forfeitures Office.

Privacy and Civil Liberties Protection

In conducting border searches, CBP officers strictly adhere to all constitutional and statutory requirements, including those that are applicable to privileged, personal, or business confidential information. CBP has strict oversight policies and procedures that implement these constitutional and statutory safeguards. Further information on DHS and CBP privacy policy can be found at www.dhs.gov/privacy.

The DHS Office for Civil Rights and Civil Liberties investigates complaints alleging a violation by DHS employees of an individual's civil rights or civil liberties. Additional information about the Office is available at www.dhs.gov/civilliberties.

Additional information on CBP's search authority, including a copy of CBP's policy on the border search of information, can be found at: www.cbp.gov/xp/cgov/travel/admissibility/.

Customer Service Contacts

Customer Service Center – This office responds to general or specific questions or concerns about CBP examinations. You may contact us in any one of three ways:

Telephone – During the hours of 8:30 a.m. to 5:00 p.m. Eastern Time:
(877) 227-5511 (toll-free call for U.S. callers)
(703) 526-4200 (international callers)
(866) 880-6582 (TDD)

Online through the "Questions" tab at: www.cbp.gov

Mail address format:
CBP Customer Service Center (Rosslyn VA)
1300 Pennsylvania Avenue NW
Washington, D.C. 20229

Please visit the U.S. Customs and Border Protection Website at www.cbp.gov

Privacy Act Statement

Pursuant to 5 U.S.C. § 552a (e)(3), this Privacy Act Statement serves to inform you of the following concerning the possible collection of information from your electronic device.

AUTHORITY and PURPOSE: See above, **Purpose for and Authority to Search.**

ROUTINE USES: The subject information may be made available to other agencies for investigation and/or for obtaining assistance relating to jurisdictional or subject matter expertise, or for translation, decryption, or other technical assistance. This information may also be made available to assist in border security and intelligence

activities, domestic law enforcement and the enforcement of other crimes of a transnational nature, and shared with elements of the federal government responsible for analyzing terrorist threat information.

CONSEQUENCES OF FAILURE TO PROVIDE INFORMATION: Collection of this information is mandatory at the time that CBP or ICE seeks to copy information from the electronic device. Failure to provide information to assist CBP or ICE in the copying of information from the electronic device may result in its detention and/or seizure.

Attachment 1

CBP Directive

CBP DIRECTIVE NO. 3340-049 DATE: August 20, 2009

ORIGINATING OFFICE: FO:TO

SUPERSEDES:

REVIEW DATE: August 2012

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION

1 PURPOSE. To provide guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices, encountered by U.S. Customs and Border Protection (CBP) at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.

These searches are part of CBP's long-standing practice and are essential to enforcing the law at the U.S. border. Searches of electronic devices help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, contraband, and child pornography. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark and export control violations. Finally, searches at the border are often integral to a determination of admissibility under the immigration laws.

2 POLICY.

2.1 CBP will protect the rights of individuals against unreasonable search and seizure and ensure privacy protections while accomplishing its enforcement mission.

2.2 All CBP Officers, Border Patrol Agents, Air Interdiction Agents, Marine Interdiction Agents, and other employees authorized by law to perform searches at the border, the functional equivalent of the border (FEB), or the extended border shall adhere to the policy described in this Directive.

2.3 This Directive governs border search authority only. It does not limit CBP's authority to conduct other lawful searches at the border, e.g., pursuant to a warrant, consent, or incident to an arrest; it does not limit CBP's ability to record impressions relating to border encounters; it does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.4 This Directive does not govern searches of shipments containing commercial quantities of electronic devices (e.g., a shipment of hundreds of laptop computers transiting from the factory to the distributor).

2.5 This Directive does not supersede *Restrictions on Importation of Seditious Matter*, Directive 2210-001A. Seditious materials encountered through a border search should continue to be handled pursuant to Directive 2210-001A or any successor thereto.

2.6 This Directive does not supersede *Processing Foreign Diplomatic and Consular Officials*, Directive 3340-032. Diplomatic and consular officials encountered at the border, the FEB, or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.7 This Directive applies to searches performed by or at the request of CBP. With respect to searches performed by U.S. Immigration and Customs Enforcement (ICE), ICE Special Agents exercise concurrently-held border search authority that is covered by ICE's own policy and procedures. When CBP detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

3 DEFINITIONS.

3.1 Officer. A Customs and Border Protection Officer, Border Patrol Agent, Air Interdiction Agent, Marine Interdiction Agent, Internal Affairs Agent, or any other official of CBP authorized to conduct border searches.

3.2 Electronic Device. Includes any devices that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music and other media players, and any other electronic or digital devices.

3.3 Destruction. For electronic records, destruction is deleting, overwriting, or degaussing in compliance with CBP Information Systems Security Policies and Procedures Handbook, CIS HB 1400-05C.

3.4 Border Search of Information. Excludes actions taken to determine if a device functions (e.g., turning an electronic device on and off), or actions taken to determine if contraband is concealed within the device itself. The definition also excludes the review of information voluntarily provided by an individual in an electronic format (for example, when an individual voluntarily shows an e-ticket on an electronic device to an Officer).

4 AUTHORITY/REFERENCES. 8 U.S.C. 1225, 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. 401 and other laws relating to exports; Guidelines for Detention and Seizures of Pornographic Materials, Directive 4410-001B; Disclosure of Business Confidential Information to Third Parties, Directive 1450-015; Accountability and Control of Custody Receipt for Detained and Seized Property (CF6051), Directive 5240-005.

5 PROCEDURES.

5.1 Border Searches.

5.1.1 Border searches may be performed by an Officer or other individual authorized to perform or assist in such searches (e.g., under 19 U.S.C. 507).

5.1.2 In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border, subject to the requirements and limitations provided herein and applicable law.

5.1.3 Searches of electronic devices will be documented in appropriate CBP systems of records and should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire search, or where a supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof.

5.1.4 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, or other operational considerations that make it inappropriate to permit the individual to remain present. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement techniques or potentially compromise other operational considerations, the individual will not be permitted to observe the search itself.

5.2 Review and Handling of Privileged or Other Sensitive Material.

5.2.1 Officers may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work product privilege. Legal materials are not necessarily exempt from a border search, but they may be subject to the following special handling procedures: If an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate.

5.2.2 Other possibly sensitive information, such as medical records and work-related information carried by journalists, shall be handled in accordance with any applicable federal law and CBP policy. Questions regarding the review of these materials shall be directed to the CBP Associate/Assistant Chief Counsel, and this consultation shall be noted in appropriate CBP systems of records.

5.2.3 Officers encountering business or commercial information in electronic devices shall treat such information as business confidential information and shall protect that information from unauthorized disclosure. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws, as well as CBP policies, may govern or restrict the handling of the information. Any questions regarding the handling of business or commercial information may be directed to the CBP Associate/Assistant Chief Counsel.

5.2.4 Information that is determined to be protected by law as privileged or sensitive will only be shared with federal agencies that have mechanisms in place to protect appropriately such information.

5.3 Detention and Review in Continuation of Border Search of Information

5.3.1 Detention and Review by CBP

An 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.

5.3.1.1 Approval of and Time Frames for Detention. 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, 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, 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 of records.

5.3.1.2 Destruction. Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.3, there is not probable cause to seize it, any copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is 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 of records and which must be no later than twenty one (21) days after such determination. The destruction shall be noted in appropriate CBP systems of records.

5.3.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, and when the fact of conducting this search can be disclosed to the individual transporting the device without hampering national security or

law enforcement or other operational considerations, the individual may be notified of the purpose and authority for these types of searches, 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.

5.3.1.4 Custody Receipt. If CBP determines it is necessary to detain temporarily an electronic device to continue the search, the Officer detaining the device shall issue a completed Form 6051D to the individual prior to the individual's departure.

5.3.2 Assistance by Other Federal Agencies.

5.3.2.1 The use of other federal agency analytical resources outside of CBP and ICE, such as translation, decryption, and subject matter expertise, may be needed to assist CBP in reviewing the information contained in electronic devices or to determine the meaning, context, or value of information contained in electronic devices.

5.3.2.2 Technical Assistance – With or Without Reasonable Suspicion. Officers may sometimes have technical difficulties in conducting the search of electronic devices such that technical assistance is needed to continue the border search. Also, in some cases Officers may encounter information in electronic devices that requires technical assistance to determine the meaning of such information, such as, for example, information that is in a foreign language and/or encrypted (including information that is password protected or otherwise not readily reviewable). In such situations, Officers may transmit electronic devices or copies of information contained therein to seek technical assistance from other federal agencies. Officers may seek such assistance with or without individualized suspicion.

5.3.2.3 Subject Matter Assistance by Other Federal Agencies – With Reasonable Suspicion. In addition to encountering information in electronic devices that is in a foreign language, encrypted, or requires technical assistance, Officers may encounter information that requires referral to subject matter experts in other federal agencies to determine the meaning, context, or value of information contained therein as it relates to the laws enforced and administered by CBP. Therefore, Officers may transmit electronic devices or copies of information contained therein to other federal agencies for the purpose of obtaining subject matter assistance when they have reasonable suspicion of activities in violation of the laws enforced by CBP. While many factors may result in reasonable suspicion, the presence of an individual on a government-operated and government-vetted terrorist watch list will be sufficient to create reasonable suspicion of activities in violation of the laws enforced by CBP.

5.3.2.4 Approvals for seeking translation, decryption, and subject matter assistance. Requests for translation, decryption, and subject matter assistance require supervisory approval and shall be properly documented and recorded in CBP systems of records. If an electronic device is to be detained after the individual's departure, the Officer detaining the device shall execute a Form 6051D and provide a copy to the individual

prior to the individual's departure. All transfers of the custody of the electronic device will be recorded on the Form 6051D.

5.3.2.5 Electronic devices should be transmitted only when necessary to render the requested translation, decryption, or subject matter assistance. Otherwise, a copy of such information should be transmitted in lieu of the device in accord with this Directive.

5.3.2.6 When information from an electronic device is transmitted to another federal agency for translation, decryption, or subject matter assistance, the individual will be notified of this transmission unless CBP determines, in consultation with the receiving agency or other agency as appropriate, that notification would be contrary to national security or law enforcement or other operational interests. If CBP's transmittal seeks assistance regarding possible terrorism, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the transmittal or his or her presence on a watch list. When notification is made to the individual, the Officer will annotate the notification in CBP systems of records and on the Form 6051D.

5.3.3 Responses and Time for Assistance

5.3.3.1 Responses Required. Agencies receiving a request for assistance in conducting a border search are to provide such assistance as expeditiously as possible. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced by CBP.

5.3.3.2 Time for Assistance. Responses from assisting agencies are expected in an expeditious manner so that CBP may complete the border search in a reasonable period of time. Unless otherwise approved by the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager, responses from an assisting agency should be received within fifteen (15) days. If the assisting agency is unable to respond in that period of time, the Director Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager may permit extensions in increments of seven (7) days.

5.3.3.3 Revocation of a Request for Assistance. If at any time a CBP supervisor involved in a request for assistance is not satisfied with the assistance being provided, the timeliness of assistance, or any other articulable reason, the request for assistance may be revoked, and the CBP supervisor may require the assisting agency to return to CBP all electronic devices that had been provided to the assisting agency, and any copies thereof, as expeditiously as possible, except as noted in 5.4.2.3. Any such revocation shall be documented in appropriate CBP systems of records. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency pursuant to the procedures outlined in this Directive.

5.3.3.4 Destruction. Except as noted in section 5.4.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the information does not exist, CBP will retain no copies of the information.

5.4 Retention and Sharing of Information Found in Border Searches

5.4.1 Retention and Sharing of Information Found in Border Searches

5.4.1.1 Retention with Probable Cause. 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 thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce.

5.4.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. 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 privacy and data protection standards of the system of records in which such information is retained. For example, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or ENFORCE or other systems as may be appropriate and consistent with the policies governing such systems.

5.4.1.3 Sharing Generally. Nothing in this Directive limits the authority of CBP to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, and foreign law enforcement agencies to the extent consistent with applicable law and policy.

5.4.1.4 Sharing of Terrorism Information. Nothing in this Directive is intended to limit the sharing of terrorism-related information to the extent the sharing of such information is mandated by statute, Presidential Directive, or DHS policy. Consistent with 6 U.S.C. 122(d)(2) and other applicable law and policy, CBP, as a component of DHS, will promptly share any terrorism information encountered in the course of a border search with elements of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the element receiving the information will be responsible for providing CBP with all appropriate findings, observations, and conclusions relating to the laws enforced by CBP. The receiving entity will be responsible for managing retention and disposition of information it receives in accordance with its own legal authorities and responsibilities.

5.4.1.5 Safeguarding Data During Storage and Transmission. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during transmission to another federal agency. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during transmission 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 or equivalent level manager and the CBP Office of Internal Affairs.

5.4.1.6 Destruction. Except as noted in this section or elsewhere in this Directive, if after reviewing information, there exists no probable cause to seize the information, CBP will retain no copies of the information.

5.4.2 Retention by Agencies Providing Translation, Decryption, or Subject Matter Assistance

5.4.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting federal agency may be retained by that agency for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.4.2.3 below.

5.4.2.2 Return or Destruction. At the conclusion of the requested assistance, all information must be returned to CBP as expeditiously as possible, and the assisting agency must advise CBP in accordance with section 5.3.3 above. In addition, the assisting federal agency should destroy all copies of the information transferred to that agency unless section 5.4.2.3 below applies. In the event that any electronic devices are transmitted, they must not be destroyed; they are to be returned to CBP unless seized by the assisting agency based on probable cause or retained per 5.4.2.3.

5.4.2.3 Retention with Independent Authority. If an assisting federal agency elects to continue to retain or seize an electronic device or information contained therein, that agency shall assume responsibility for processing the retention or seizure. Copies may be retained by an assisting federal agency 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 agency is authorized by law to receive and analyze such information. In such cases, the retaining agency should advise CBP of its decision to retain information under its own authority.

5.5 Reporting Requirements

5.5.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or 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.

5.5.2 In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.3.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

5.5.3 Reporting requirements for this Directive are in addition to, and do not replace, any other applicable reporting requirements.

5.6 Management Requirements

5.6.1 The duty supervisor shall ensure that the Officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

5.6.2 The appropriate CBP Second line supervisor shall approve and monitor the status of the detention of all electronic devices or copies of information contained therein.

5.6.3 The appropriate CBP Second line supervisor shall approve and monitor the status of the transfer of any electronic device or copies of information contained therein for translation, decryption, or subject matter assistance from another federal agency.

5.6.4 The Director, Field Operations, Chief Patrol Agent, Director, Air Operations, Director, Marine Operations, or equivalent level manager shall establish protocols to monitor the proper documentation and recording of searches conducted pursuant to this Directive and the detention, transfer, and final disposition of electronic devices or copies of information contained therein in order to ensure compliance with the procedures outlined in this Directive.

6 MEASUREMENT. 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 pursuant to this Directive.

7 AUDIT. CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

8 NO PRIVATE RIGHT CREATED. This Directive is an internal policy statement of U.S. Customs and Border Protection and does not create or confer any rights, privileges, or benefits on any person or party.

9 DISCLOSURE. This Directive may be shared with the public.

10. SUPERSEDES. Procedures for Border Search/Examination of Documents, Paper, and Electronic Information (July 5, 2007) and Policy Regarding Border Search of Information (July 16, 2008) to the extent they pertain to electronic devices.

Acting Commissioner
U.S. Customs and Border Protection

Attachment 2

ICE Directive

DISTRIBUTION: ICE
DIRECTIVE NO.: 7-6.1
ISSUE DATE: August 18, 2009
EFFECTIVE DATE: August 18, 2009
REVIEW DATE: August 18, 2012
SUPERSEDES: See Section 3 Below.

DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES

1. PURPOSE and SCOPE.

1.1. This Directive provides legal guidance and establishes policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE. This Directive applies to searches of electronic devices of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise.

1.2. This Directive applies to border search authority only. Nothing in this Directive limits the authority of ICE Special Agents to act pursuant to other authorities such as a warrant, a search incident to arrest, or a routine inspection of an applicant for admission.

2. AUTHORITIES/REFERENCES. 8 U.S.C. § 1357 and other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1589a, 1595a(d), and other pertinent provisions of customs laws and regulations; 31 U.S.C. § 5317 and other pertinent provisions relating to monetary instruments; 22 U.S.C. § 401 and other laws relating to exports; and the December 12, 2008, ICE Office of Investigations (OI) guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices."

3. SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES. ICE Directive No. 7-6.0 entitled "Border Searches of Documents and Electronic Media" is hereby superseded as it relates to electronic devices. Additionally, all other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded as they relate to searches of electronic devices, with the exception of the March 5, 2007, OI guidance entitled "Field Guidance on Handling Detained or Seized Electronic Media from Persons of National Security Interest at Ports of Entry" and the December 12, 2008, OI guidance entitled "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media."

4. **BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

5. **DEFINITIONS.** The following definitions are provided for the purposes of this Directive:

5.1. Assistance. The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.

5.2. Electronic Devices. Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.

6. **POLICY.**

6.1. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.

6.2. When U.S. Customs and Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.

6.3. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.

7. **RESPONSIBILITIES.**

7.1. The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.

7.2. Special Agents in Charge (SACs) and Attachés are responsible for:

1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;

2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and

3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)

7.3. Attachés are responsible for ensuring coordination with their host countries, as appropriate, before conducting any such border search outside of the United States.

7.4. When ICE receives electronic devices, or copies of information therefrom, from CBP for analysis and investigation, ICE Special Agents are responsible for advising CBP of the status of any such analysis within 10 calendar days, and periodically thereafter, so that CBP records may be updated as appropriate. For example, "search ongoing"; "completed with negative results"; "returned to traveler"; or "seized as evidence of a crime."

7.5. Special Agents are responsible for complying with the provisions of this Directive, knowing the limits of ICE authority, using this authority judiciously, and ensuring comprehension and completion of any training programs relevant to border searches of electronic devices as may be required by ICE.

8. PROCEDURES.

8.1. Border Searches by ICE Special Agents.

1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.

2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement

techniques or potentially compromise other operational concerns, the individual will not be permitted to observe the search.

3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.

4) Continuation of the Border Search. At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).

5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

8.2. Chain of Custody.

1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.

2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.

3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.

4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

8.3. Duration of Border Search.

1) Special Agents are to complete the search of detained electronic devices, or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search. Searches are generally to be completed within 30 calendar days of

the date of detention, unless circumstances exist that warrant more time. Such circumstances must be documented in the appropriate ICE systems. Any detention exceeding 30 calendar days must be approved by a Group Supervisor or equivalent, and approved again every 15 calendar days thereafter, and the specific justification for additional time documented in the appropriate ICE systems.

2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the results of the assistance are received in a reasonable time (see Section 8.4(5)).

3) In determining "reasonable time," courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:

   a) The amount of information needing review;

   b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;

   c) Whether assistance was sought and the type of such assistance;

   d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;

   e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and

   f) Any unanticipated exigency that may arise.

8.4. Assistance by Other Federal Agencies and Non-Federal Entities.

1) Translation, Decryption, and Other Technical Assistance.

   a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.

   b) Special Agents may demand such assistance absent individualized suspicion.

   c) Special Agents shall document such demands in appropriate ICE systems.

2) Subject Matter Assistance.

   a) During a border search, Special Agents may encounter information in electronic devices that are not in a foreign language or encrypted, or that do not require other technical assistance, in accordance with Section 8.4(1), but that nevertheless requires referral to subject matter experts to determine whether the information is relevant to the laws enforced and administered by ICE. For the purpose of obtaining such subject matter expertise, Special Agents may create and transmit a copy of such information to other Federal agencies or non-Federal entities.

   b) Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.

   c) Special Agents shall document such demands in appropriate ICE systems.

3) Demand Letter. Unless otherwise governed by a Memorandum of Understanding or similar mechanism, each demand for assistance is to be in writing (e.g., letter or email), approved by a supervisor, and documented in the appropriate ICE systems. Demands are to detail the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing of any information found during the assistance, and relevant timeframes, including those described in this Directive.

4) Originals. For the purpose of obtaining subject matter assistance, Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Original electronic devices should be transmitted only when necessary to render the demanded assistance.

5) Time for Assistance and Responses Required.

   a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.

   b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:

      i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;

      ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;

iv) Remain in communication with the assisting agency or entity until results are received;

v) Document all communications and actions in appropriate ICE systems; and

vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

8.5. Retention, Sharing, Safeguarding, And Destruction.

1) By ICE

a) Seizure and Retention with Probable Cause. When Special Agents determine there is probable cause of unlawful activity—based on a review of information in electronic devices or on other facts and circumstances—they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.

b) Retention of Information in ICE Systems. To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.

c) Sharing. Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.

d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.

e) Destruction. Copies of information from electronic devices, or portions thereof, determined to be of no relevance to ICE will be destroyed in accordance with ICE policy governing the particular form of information. Such destruction must be accomplished by the responsible Special Agent within seven business days after conclusion of the border search unless circumstances require additional time, which must be approved by a supervisor and documented in appropriate ICE systems. All destructions must be accomplished no later than 21 calendar days after conclusion of the border search.

2) By Assisting Agencies

a) Retention during Assistance. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.

b) Return or Destruction. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.

c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

3) By Non-Federal Entities

a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.

b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

8.6. Review, Handling, and Sharing of Certain Types of Information.

1) Border Search. All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.

2) Types of Information

a) Business or Commercial Information. If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.

b) Legal Information. Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.

c) Other Sensitive Information. Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.

3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

8.7 Measurement. ICE Headquarters will develop appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from ICE systems using data elements entered by Special Agents pursuant to this Directive.

8.8 **Audit.** ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

9. **ATTACHMENTS.** None.

10. **NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved 

John Morton
Assistant Secretary
U.S. Immigration and Customs Enforcement