

Page 631

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 632

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 633

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 634

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 635

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 636

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 637

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 638

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 639

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 640

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 641

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 642

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 643

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 644

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 645

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 646

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 647

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 648

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 649

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 650

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 651

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 652

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 653

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 654

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 655

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 656

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 657

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 658

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 659

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 660

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 661

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 662

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 663

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 664

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 665

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 666

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 667

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 668

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 669

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 670

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 671

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 672

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 673

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 674

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 675

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 676

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 677

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 678

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 679

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 680

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 681

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 682

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

## U.S. CUSTOMS AND BORDER PROTECTION

**CBP DIRECTIVE NO.** 3340-049A

**DATE:** January 4, 2018

**ORIGINATING OFFICE:** FO:TO

**SUPERSEDES:** Directive 3340-049

**REVIEW DATE:** January 2021

### **SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES**

**1 PURPOSE.** 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 U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They 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. They 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 and provide additional information relevant to 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 and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or 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 (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP's authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; 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., an importation 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 functional equivalent of the border (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), Homeland Security Investigations (HSI) 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 conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

### 3 DEFINITIONS

3.1 **Officer.** A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 **Electronic Device.** 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.

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.

**4 AUTHORITY/REFERENCES.** 6 U.S.C. §§ 122, 202, 211; 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, 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; 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.

The plenary 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." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "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.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "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." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). 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. *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. 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).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *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"). 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. *See Boumelhem*, 339 F.3d at 423.

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. *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.”). 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. 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.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP’s broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

## **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 Border searches of electronic devices may 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, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should 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.

5.1.3 **Basic Search.** Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. 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.

5.1.4 **Advanced Search.** An advanced search is 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.

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

5.1.6 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.

## **5.2 Review and Handling of Privileged or Other Sensitive Material**

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP 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 composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP 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 CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

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 office, and this consultation shall be noted in appropriate CBP systems.

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 office or the CBP Privacy Officer, as appropriate.

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

### **5.3 Review and Handling of Passcode-Protected or Encrypted Information**

5.3.1 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. Passcodes or other means of access may be requested and retained as needed 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 in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 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, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

## **5.4 Detention and Review in Continuation of Border Search of Information**

### **5.4.1 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. 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.

5.4.1.1 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; 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.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, 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. 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. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified 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.

**5.4.1.4 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.

## **5.4.2 Assistance**

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

**5.4.2.1 Technical Assistance.** Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

**5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern.** Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

**5.4.2.3 Approvals for Seeking Assistance.** Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. 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.

**5.4.2.4** Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

**5.4.2.5** When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, 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 and on the Form 6051D.

### 5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected 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 or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities 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; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 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 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 or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

## 5.5 Retention and Sharing of Information Found in Border Searches

### 5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 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 from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 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 applicable system of records notice. 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 E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 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.

5.5.1.4 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 authorized 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 entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity 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.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. 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 CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 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.

## 5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

**5.5.2.3 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 assumes 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.

## **5.6 Reporting Requirements**

**5.6.1** 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.

**5.6.2** In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

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

## **5.7 Management Requirements**

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

**5.7.2** 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.

**5.7.3** 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 agency or entity.

**5.7.4** The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; 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.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

**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 REVIEW.** This Directive shall be reviewed and updated, as necessary, at least every three years.

**10 DISCLOSURE.** This Directive may be shared with the public.

**11 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; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).



Acting Commissioner

## U.S. CUSTOMS AND BORDER PROTECTION

**CBP DIRECTIVE NO.** 3340-049A

**DATE:** January 4, 2018

**ORIGINATING OFFICE:** FO:TO

**SUPERSEDES:** Directive 3340-049

**REVIEW DATE:** January 2021

### **SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES**

**1 PURPOSE.** 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 U.S. Customs and Border Protection (CBP). These searches are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer.

These searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and to protecting border security. They 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. They 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 and provide additional information relevant to 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 and Marine Agents, Office of Professional Responsibility Agents, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda or musters.

2.3 This Directive governs border searches of electronic devices – including any inbound or outbound search pursuant to longstanding border search authority and conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy. For purposes of this Directive, this excludes actions taken to determine if a device functions (e.g., turning a device on and off); or 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 (e.g., when an individual shows an e-ticket on an electronic device to an Officer, or when an alien proffers information to establish admissibility). This Directive does not limit CBP’s authority to conduct other lawful searches of electronic devices, such as those performed pursuant to a warrant, consent, or abandonment, or in response to exigent circumstances; 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., an importation 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 functional equivalent of the border (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), Homeland Security Investigations (HSI) 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 conveys such to ICE for analysis, investigation, and disposition (with appropriate documentation), the conveyance to ICE is not limited by the terms of this Directive, and ICE policy will apply upon receipt by ICE.

### **3 DEFINITIONS**

3.1 **Officer.** A Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Special Agent, or any other official of CBP authorized to conduct border searches.

3.2 **Electronic Device.** 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.

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.

**4 AUTHORITY/REFERENCES.** 6 U.S.C. §§ 122, 202, 211; 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, 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; 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.

The plenary 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." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). "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.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). "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." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). 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. *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. 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).

As a constitutional matter, border search authority is premised in part on a reduced expectation of privacy associated with international travel. *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"). 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. *See Boumelhem*, 339 F.3d at 423.

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. *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.”). 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. 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.

CBP must conduct border searches of electronic devices in accordance with statutory and regulatory authorities and applicable judicial precedent. CBP’s broad authority to conduct border searches is well-established, and courts have rejected a categorical exception to the border search doctrine for electronic devices. Nevertheless, as a policy matter, this Directive imposes certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure that the authority for border search of electronic devices is exercised judiciously, responsibly, and consistent with the public trust.

## **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 Border searches of electronic devices may 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, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should 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.

5.1.3 **Basic Search.** Any border search of an electronic device that is not an advanced search, as described below, may be referred to as a basic search. 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.

5.1.4 **Advanced Search.** An advanced search is 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.

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

5.1.6 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.

## **5.2 Review and Handling of Privileged or Other Sensitive Material**

5.2.1 Officers encountering information they identify as, or that is asserted to be, protected by the attorney-client privilege or attorney work product doctrine shall adhere to the following procedures.

5.2.1.1 The Officer shall seek clarification, if practicable in writing, from the individual asserting this privilege as to specific files, file types, folders, categories of files, attorney or client names, email addresses, phone numbers, or other particulars that may assist CBP in identifying privileged information.

5.2.1.2 Prior to any border search of files or other materials over which a privilege has been asserted, the Officer will contact the CBP Associate/Assistant Chief Counsel office. In coordination with the CBP 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 composed of legal and operational representatives, or through another appropriate measure with written concurrence of the CBP Associate/Assistant Chief Counsel office.

5.2.1.3 At the completion of the CBP 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 CBP Associate/Assistant Chief Counsel office solely for purposes of complying with a litigation hold or other requirement of law.

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 office, and this consultation shall be noted in appropriate CBP systems.

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 office or the CBP Privacy Officer, as appropriate.

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

### **5.3 Review and Handling of Passcode-Protected or Encrypted Information**

5.3.1 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. Passcodes or other means of access may be requested and retained as needed 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 in accordance with this Directive.

5.3.2 Passcodes and other means of access obtained during the course of a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search, will be deleted or destroyed when no longer needed to facilitate the search of a given device, and may not be utilized to access information that is only stored remotely.

5.3.3 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, in accordance with section 5.4 below, detain the device pending a determination as to its admissibility, exclusion, or other disposition.

5.3.4 Nothing in this Directive limits CBP's ability, with respect to any device presented in a manner that is not readily accessible for inspection, to seek technical assistance, or to use external equipment or take other reasonable measures, or in consultation with the CBP Associate/Assistant Chief Counsel office to pursue available legal remedies, to render a device in a condition that allows for inspection of the device and its contents.

#### **5.4 Detention and Review in Continuation of Border Search of Information**

##### **5.4.1 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. 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.

5.4.1.1 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; 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.

5.4.1.2 Destruction. Except as noted in section 5.5 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.4, 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. 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. The destruction shall be noted in appropriate CBP systems.

5.4.1.3 Notification of Border Search. When a border search of information is conducted on an electronic device, the individual subject to search will be notified 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.

**5.4.1.4 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.

## **5.4.2 Assistance**

Officers may request assistance that may be needed to access and search an electronic device and the information stored therein. Except with respect to assistance sought within CBP or from ICE, the following subsections of 5.4.2 govern requests for assistance.

**5.4.2.1 Technical Assistance.** Officers may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection. For example, Officers may encounter a device or information that is not readily accessible for inspection due to encryption or password protection. Officers may also require translation assistance to inspect information that is in a foreign language. In such situations, Officers may convey electronic devices or copies of information contained therein to seek technical assistance.

**5.4.2.2 Subject Matter Assistance – With Reasonable Suspicion or National Security Concern.** Officers may encounter information that requires referral to subject matter experts to determine the meaning, context, or value of information contained therein as it relates to the laws enforced or administered by CBP. Therefore, Officers may convey electronic devices or copies of information contained therein for the purpose of obtaining subject matter assistance when there is a national security concern or they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP.

**5.4.2.3 Approvals for Seeking Assistance.** Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. 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.

**5.4.2.4** Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of data from the device should be conveyed in lieu of the device in accordance with this Directive.

**5.4.2.5** When an electronic device or information contained therein is conveyed for assistance, the individual subject to search will be notified of the conveyance unless the Officer or other appropriate CBP official determines, in consultation with the receiving agency or other entity as appropriate, that notification would impair national security, law enforcement, officer safety, or other operational interests. If CBP seeks assistance for counterterrorism purposes, if a relevant national security-related lookout applies, or if the individual is on a government-operated and government-vetted terrorist watch list, the individual will not be notified of the conveyance, the existence of a relevant national security-related lookout, 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 and on the Form 6051D.

### 5.4.3 Responses and Time for Assistance

5.4.3.1 Responses Required. Agencies or entities receiving a request for assistance in conducting a border search are expected 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 or administered by CBP.

5.4.3.2 Time for Assistance. Responses from assisting agencies or entities 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; Special Agent in Charge; or equivalent level manager, responses should be received within fifteen (15) days. If the assisting agency or entity is unable to respond in that period of time, the Director Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager may permit extensions in increments of seven (7) days.

5.4.3.3 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 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 or entity to return to CBP all electronic devices provided, and any copies thereof, as expeditiously as possible, except as noted in 5.5.2.3. Any such revocation shall be documented in appropriate CBP systems. When CBP has revoked a request for assistance because of the lack of a timely response, CBP may initiate the request with another agency or entity pursuant to the procedures outlined in this Directive.

5.4.3.4 Destruction. Except as noted in section 5.5.1 below or elsewhere in this Directive, if after reviewing information, probable cause to seize the device or the information from the device does not exist, CBP will retain no copies of the information.

## 5.5 Retention and Sharing of Information Found in Border Searches

### 5.5.1 Retention and Sharing of Information Found in Border Searches

5.5.1.1 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 from the device, contains evidence of a violation of law that CBP is authorized to enforce or administer.

5.5.1.2 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 applicable system of records notice. 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 E3 or other systems as may be appropriate and consistent with the policies governing such systems.

5.5.1.3 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.

5.5.1.4 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 authorized 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 entities of the federal government responsible for analyzing terrorist threat information. In the case of such terrorism information sharing, the entity 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.

5.5.1.5 Safeguarding Data During Storage and Conveyance. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during conveyance. 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 CBP Office of Professional Responsibility and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

5.5.1.6 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.

## 5.5.2 Retention by Agencies or Entities Providing Technical or Subject Matter Assistance

5.5.2.1 During Assistance. All electronic devices, or copies of information contained therein, provided to an assisting agency or entity may be retained for the period of time needed to provide the requested assistance to CBP or in accordance with section 5.5.2.3 below.

5.5.2.2 Return or Destruction. CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible, and that the assisting agency or entity advise CBP in accordance with section 5.4.3 above. In addition, the assisting agency or entity should destroy all copies of the information conveyed unless section 5.5.2.3 below applies. In the event that any electronic devices are conveyed, they must not be destroyed;

they are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.2.3.

**5.5.2.3 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 assumes 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.

## **5.6 Reporting Requirements**

**5.6.1** 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.

**5.6.2** In instances where an electronic device or copy of information contained therein is forwarded within CBP as noted in section 5.4.1, the receiving Officer is responsible for recording all information related to the search from the point of receipt forward through the final disposition.

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

## **5.7 Management Requirements**

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

**5.7.2** 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.

**5.7.3** 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 agency or entity.

**5.7.4** The Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; 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.

5.7.5 Officers will ensure, in coordination with field management as appropriate, that upon receipt of any subpoena or other request for testimony or information regarding the border search of an electronic device in any litigation or proceeding, notification is made to the appropriate CBP Associate/Assistant Chief Counsel office.

**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.

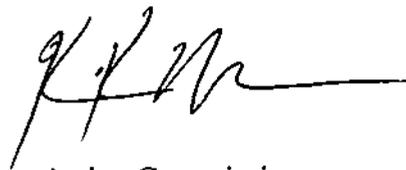
**7 AUDIT.** CBP Management Inspection will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.

**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 REVIEW.** This Directive shall be reviewed and updated, as necessary, at least every three years.

**10 DISCLOSURE.** This Directive may be shared with the public.

**11 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; CBP Directive No. 3340-049, Border Searches of Electronic Devices Containing Information (August 20, 2009).



Acting Commissioner



**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.<sup>1</sup> 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,<sup>2</sup> 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.<sup>3</sup>

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

---

<sup>1</sup> 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.

<sup>2</sup> 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](http://www.dhs.gov/privacy)).

<sup>3</sup> 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.

<sup>4</sup> *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* [www.dhs.gov/privacy](http://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.<sup>5</sup> 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.<sup>6</sup> 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.

---

<sup>5</sup> See DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>6</sup> 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.<sup>7</sup> 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"<sup>8</sup>). 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.<sup>9</sup>

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

---

<sup>7</sup> 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.

<sup>8</sup> 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.

<sup>9</sup> 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](http://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<sup>10</sup> 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<sup>11</sup> 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.

<sup>10</sup> See <https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf>.

<sup>11</sup> See DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), available at [www.dhs.gov/privacy](http://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.”<sup>12</sup>

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.<sup>13</sup>

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

<sup>12</sup> CBP Directive No. 3340-049A at 5.1.3.

<sup>13</sup> 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.<sup>14</sup>

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.<sup>15</sup>

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.

---

<sup>14</sup> 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.

<sup>15</sup> 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.<sup>16</sup> For both basic and advanced searches, Officers may not intentionally use the device to access information that is solely stored remotely.<sup>17</sup> 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.<sup>18</sup>

## *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

<sup>16</sup> CBP Directive No. 3340-049A at 5.1.2.

<sup>17</sup> CBP Directive No. 3340-049A at 5.1.2.

<sup>18</sup> CBP Directive No. 3340-049A at 5.1.2.



privileged information.<sup>19</sup> 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.<sup>20</sup> 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.<sup>21</sup>

#### *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.<sup>22</sup> 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.<sup>23</sup> The CBP Privacy Officer shall conduct a CBP Privacy Evaluation of this requirement

<sup>19</sup> CBP Directive No. 3340-049A at 5.2.1.1.

<sup>20</sup> CBP Directive No. 3340-049A at 5.2.1.2.

<sup>21</sup> CBP Directive No. 3340-049A at 5.2.1.3.

<sup>22</sup> CBP Directive No. 3340-049A at 5.3.1.

<sup>23</sup> 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)<sup>24</sup> 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<sup>25</sup> 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,

<sup>24</sup> See DHS/CBP/PIA-006 Automated Targeting System (ATS), available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>25</sup> 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.<sup>26</sup>

## 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

---

<sup>26</sup> 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](http://www.dhs.gov/privacy).



detention and search. CBP has created a tear-sheet<sup>27</sup> 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.<sup>28</sup>

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.<sup>29</sup>

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<sup>30</sup> 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<sup>31</sup> 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)<sup>32</sup> 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.

<sup>27</sup> See <https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf>.

<sup>28</sup> See CBP Search Authority, available at <https://www.cbp.gov/travel/cbp-search-authority>.

<sup>29</sup> CBP Directive at 5.4.1.3.

<sup>30</sup> DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297.

<sup>31</sup> DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778.

<sup>32</sup> 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,<sup>33</sup> are subject to search by CBP pursuant to its

<sup>33</sup> 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.<sup>34</sup> 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."<sup>35</sup> "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.'<sup>36</sup> "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."<sup>37</sup> 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.<sup>38</sup>

<sup>34</sup> CBP Directive No. 3340-049A at 5.2.1.1 (regarding privilege) and at 5.3.1 (regarding passcodes and encryption).

<sup>35</sup> *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004).

<sup>36</sup> *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

<sup>37</sup> *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

<sup>38</sup> *See, e.g., United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. Oduyayo*, 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.<sup>39</sup> 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.<sup>40</sup>

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.<sup>41</sup> 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.<sup>42</sup>

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).

<sup>39</sup> 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").

<sup>40</sup> See *Boumelhem*, 339 F.3d at 423.

<sup>41</sup> 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.").

<sup>42</sup> 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.<sup>43</sup> 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.<sup>44</sup> 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,<sup>45</sup> and other systems of records are kept with annotations noting the time they were added to the file for contextual relevancy.

---

<sup>43</sup> CBP Directive No. 3340-049A at 5.3.1.

<sup>44</sup> CBP Directive No. 3340-049A at 5.3.2.

<sup>45</sup> 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.<sup>46</sup> 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<sup>47</sup> when appropriate, and creation and/or

<sup>46</sup> CBP Directive No. 3340 at 5.5.1.5.

<sup>47</sup> 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.<sup>48</sup>

**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<sup>49</sup> 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

---

<sup>48</sup> 6 U.S.C. § 211(k)(5).

<sup>49</sup> The CBP Management Inspections Division is a division of the Office of Professional Responsibility that provides internal audit and oversight for CBP operations.

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT**  
**ICE Policy System**

**DISTRIBUTION:** ICE  
**DIRECTIVE NO.:** 7-6.0  
**ISSUE DATE:** July 16, 2008  
**EFFECTIVE DATE:** July 16, 2008  
**REVIEW DATE:** July 16, 2011  
**SUPERSEDES:** See Section 3 Below.

**DIRECTIVE TITLE: BORDER SEARCHES OF DOCUMENTS AND ELECTRONIC MEDIA**

1. **PURPOSE and SCOPE.** This Directive sets forth the legal guidelines and establishes policy and procedures within ICE for border search authority to search, review, retain, and share certain documents and electronic media possessed by individuals during investigative operations at the border, the functional equivalent of the border, and the extended border. This Directive applies to all ICE personnel who meet the definition of "customs officer" under 19 U.S.C. § 1401(i) ("ICE Special Agents"), other domestic or foreign law enforcement officers cross designated by ICE as customs officers, and persons whose assistance ICE demands under 19 U.S.C. § 507 (collectively, "ICE personnel"). This Directive applies to searches of documents and electronic media of all persons arriving in, departing from, or transiting through the United States, unless specified otherwise. Each operational office will maintain appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this policy.

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

2. **AUTHORITIES/REFERENCES.**
  - 2.1 19 U.S.C. § 482, Search of vehicles and persons.
  - 2.2 19 U.S.C. § 507, Assistance for Officers.
  - 2.3 19 U.S.C. § 1401(i), Customs Officers.
  - 2.4 19 U.S.C. § 1461, Inspection of merchandise and baggage.
  - 2.5 19 U.S.C. § 1467, Special inspection, examination, and search.
  - 2.6 19 U.S.C. § 1496, Examination of baggage.
  - 2.7 19 U.S.C. § 1499, Examination of merchandise.

- 2.8 19 U.S.C. § 1581, Boarding vessels.
  - 2.9 19 U.S.C. § 1582, Search of persons and baggage; regulations.
  - 2.10 19 U.S.C. § 1583, Examination of outbound mail.
  - 2.11 19 U.S.C. § 1595, Searches and seizures.
  - 2.12 19 C.F.R. Part 145, Mail Importations.
  - 2.13 19 C.F.R. Part 162, Inspection, Search, and Seizure.
  - 2.14 8 U.S.C. § 1225, Inspection by immigration officers; expedited removal of inadmissible arriving aliens; referral for hearing.
  - 2.15 8 U.S.C. § 1357, Powers of immigration officers and employees.
  - 2.16 8 C.F.R. § 236.1(e), Privilege of Communication.
  - 2.17 31 U.S.C. § 5317, Search authority for compliance with Currency and Monetary Instruments Reporting Act.
3. **SUPERSEDED/CANCELLED POLICY/SUMMARY OF CHANGES.** Customs Directive 3340-006A, entitled “Procedures for Examining Documents and Papers,” dated February 4, 2000, and all other directives, memoranda, bulletins, manuals, handbooks, and other guidelines and procedures relating to this subject and issued by the former U.S. Customs Service or the former U.S. Immigration and Naturalization Service no longer apply to ICE. All other issuances on this subject issued by ICE prior to the date of this Directive are hereby superseded, 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.”
4. **BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, ICE Special Agents may review documents, books, pamphlets, and other printed material, as well as 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 uncovering vital law enforcement information. For example, searches of documents and electronic media are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography, illegal monetary instruments, and information in violation of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.

## 5. DEFINITIONS.

- 5.1 Assistance.** The use of third party analytic resources, outside of ICE, such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in documents and electronic media or in determining the meaning, context, or value of information contained therein.
- 5.2 Documents.** All papers and other written documentation including, but not limited to, those relating to the alien's identity and/or admissibility (e.g., passports, visas, credit cards, licenses, social security cards, evidence of direct threats, criminal terrorist or a threat to national security); those relating to the import and/or export of goods and merchandise to or from the United States; other materials such as books, pamphlets, and printed/manuscript material; monetary instruments; and written materials commonly referred to as "pocket trash" or "pocket litter."
- 5.3 Electronic Media.** Any device capable of storing information in digital or analog form. Examples include: hard drives, compact disks, digital versatile disks, flash drives, portable music players, cell phones, pagers, beepers, and video and audio tapes and disks.
- 5.4 Letter Class Mail.** U.S. first class mail and its international equivalent. This includes postcards, aerogrammes, letter packets, etc., mailed at the letter class rate or equivalent class or category of postage. To be considered first class mail, a letter must be presently in the U.S. postal system. Only articles presently within the U.S. postal system are deemed "mail," even if they are stamped. Letters that are to be mailed, whether carried or in baggage, are not considered to be letter class mail.
- 6. POLICY.** ICE Special Agents acting under border search authority may search, detain, seize, retain, and share documents and electronic media consistent with the guidelines and applicable laws set forth herein. In the course of a border search, and absent individualized suspicion, officers can review the information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States, subject to the requirements and limitations provided herein. Assistance to complete a thorough border search may be sought from outside agencies and entities, on a case by case basis, as appropriate.

NOTE: Nothing in this policy limits the authority of ICE Special Agents to make written notes or reports or to document impressions relating to a border encounter.

## 7. RESPONSIBILITIES.

- 7.1** The Directors of OI, OPR, and OIA have oversight over the implementation of the provisions of this Directive.

- 7.2 Special Agents in Charge and Attachés are responsible for implementing the provisions of this Directive and ensuring that their subordinates receive a copy of this Directive and are familiar with its contents.
- 7.3 Attachés are responsible for ensuring coordination with their host countries and representative Ambassadors, as appropriate, before conducting any such border search outside of the United States.
- 7.4 ICE personnel are responsible for complying with the provisions of this Directive and must know the limits of ICE authority and use this authority judiciously.

## 8. PROCEDURES.

### 8.1 Border Searches by ICE Special Agents.

- 1) Border searches of documents and electronic media must be performed by an ICE Special Agent or other 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) At any point during a border search, documents and electronic media, or copies thereof, 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).
- 3) Except as noted below in Section 8.5(2)(c), if, after reviewing the documents and electronic media, probable cause to seize the documents or electronic media does not exist, all detained copies must be destroyed. Any originals must be returned to the traveler as expeditiously as possible.

### 8.2 Chain of Custody.

- 1) Detentions of documents and electronic media. Whenever ICE detains documents or electronic media, or copies thereof, the Special Agent will initiate a chain of custody form (CBP 6051-D) or other appropriate documentation.
- 2) Seizures of documents and electronic media. Whenever ICE seizes documents or electronic media, or copies thereof, the seizing Special Agent is to enter the seizure into the Seized Asset and Case Tracking System (SEACATS) via the completion of a Search, Arrest, and Seizure Report (SAS). Additionally, the seizing agent must complete the appropriate chain of custody forms (Customs Form 6051) or other appropriate documentation.

### 8.3 Reasonable Time.

- 1) ICE personnel are to complete review of any detained or seized documents and electronic media in a reasonable time.
- 2) ICE Special Agents seeking assistance from other Federal agencies or entities are responsible for ensuring that the results of the review are received in a reasonable time (see Section 8.4(5)).
- 3) In determining “reasonable time,” ICE Special Agents should consider the following factors:
  - a) The nature of the documents or electronic media;
  - 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) The elapsed time between the detention, the initial border search, and the continued border search, including any assistance demand;
  - d) Whether assistance was sought and the type of such assistance;
  - e) Whether ICE followed up with the agency or entity providing assistance to ensure a timely review;
  - f) The amount of information needing review; and
  - g) Any unanticipated exigency that may arise.

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

- 1) Translation and Decryption
  - a) During a border search, ICE Special Agents may encounter information in documents or electronic media that is in a foreign language and/or encrypted. To assist ICE in determining the meaning of such information, ICE Special Agents may demand translation and/or decryption assistance from other Federal agencies or non-federal entities.
  - b) ICE Special Agents may seek such assistance absent individualized suspicion.
  - c) ICE Special Agents shall document and record such demands for translation and decryption assistance.

## 2) Subject Matter Assistance.

- a) During a border search, ICE Special Agents may encounter information in documents or electronic media that are not in a foreign language or encrypted, but that nevertheless require 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, ICE Special Agents may create and transmit a copy of information to other Federal agencies or non-federal entities.
- b) ICE Special Agents may demand such assistance when they have reasonable suspicion of activities in violation of the laws enforced by ICE.
- c) ICE Special Agents shall document and record such demands for subject matter assistance, as appropriate.

## 3) Originals. For the purpose of obtaining subject matter expertise, ICE Special Agents may create and transmit copies of information to other Federal agencies or non-Federal entities. Any original documents and media should be transmitted only when necessary to render the demanded assistance. If it is not necessary to transmit original documents and media, ICE Special Agents should return originals to the traveler immediately, barring continuing reasonable suspicion to detain.

## 4) Responses Required.

- a) ICE Special Agents shall inform assisting agencies or entities that they are to provide results of translation and decryption as expeditiously as possible. Additionally, ICE Special Agents shall ensure that assisting agencies and non-federal 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.
- b) If at any time an ICE Special Agent or his/her supervisor are not satisfied with the assistance being provided, the timeliness of assistance, or any other articulable reason, the demand for assistance should be revoked and the ICE Special Agent shall require the assisting agency or non-federal entity to return all documents and electronic media to ICE as expeditiously as possible.

## 5) Time for Assistance.

- a) Assistance should be accomplished within a reasonable period of time in order to preserve the status of the documents or electronic media and the integrity of the border search.

- b) It is the responsibility of the ICE Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities. If a demand for assistance is made outside of the Department of Homeland Security, within the first thirty days after demanding the assistance, the ICE Special Agent demanding the assistance shall contact the assisting agency or entity for a status report on the request. If the assisting agency or entity anticipates needing more than thirty days to complete its review and analysis, the ICE Special Agent demanding the assistance shall continue to communicate with the assisting agency or entity on a regular basis until the review is complete and the results have been received. The ICE Special Agent demanding the assistance shall document each communication with the assisting agency or entity. If assisting agencies or entities are not acting in a reasonable time, the ICE Special Agent demanding the assistance shall consult with a supervisor on what action is appropriate.
- c) Unless otherwise governed by a Memorandum of Understanding, or similar mechanism, each demand for assistance shall include a letter requesting assistance and detailing the context of the search requested, ICE's legal parameters regarding the search, retention, and sharing, as well as any relevant timeframes, including those described in this section.

## 8.5 RETENTION, SHARING, SAFEGUARDING AND DESTRUCTION.

### 1) By ICE.

- a) Law Enforcement Purposes. When ICE Special Agents determine there is probable cause of unlawful activity—based on a review of information in documents or electronic media or on other facts and circumstances—they may seize and retain the originals and/or copies of relevant documents or electronic media or relevant portions thereof, as authorized by law.
- b) Immigration Purposes. To the extent authorized by law, ICE may retain information relevant to immigration matters in ICE record systems. Use, retention, and sharing of such information is governed by the privacy and data protection standards of the system in which such information is retained.
- c) Sharing. Copies of documents or electronic media, 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.
- d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, 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 copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic media 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 Help Desk.

- e) Destruction. Copies of documents or electronic media, or portions thereof, determined to be of no relevance to ICE will be destroyed. Such destruction must be documented by the responsible ICE Special Agent. Any originals will be returned to the traveler as expeditiously as possible at the conclusion of the negative border search.

## 2) By Assisting Agencies and Non-Federal Entities.

- a) Retention During Assistance. All documents and electronic media, whether originals or copies, 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 documents and electronic media 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 documents or electronic media 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 documents or electronic media were transmitted, the assisting Federal agency may make a copy for its retention; however, any originals must be returned to ICE.

## 8.6 Non-Federal Entities.

- 1) ICE may provide copies of documents or electronic media 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.
- 2) 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.

## 8.7 Review and Handling of Certain Types of Information:

### 1) Attorney-Client Privilege.

- a) Occasionally, an individual claims that the attorney-client privilege prevents the search of his or her information at the border. Although legal materials are not necessarily exempt from a border search, they may be subject to special handling procedures.
- b) Correspondence, court documents, and other legal documents may be covered by attorney-client privilege. If ICE personnel 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 officer must seek advice from the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's office before conducting a search of the document.

### 2) Sealed Letter Class Mail.

- a) Border searches of mail are governed by particularized law and policy. *See* 19 C.F.R. Part 145; 19 U.S.C. § 1583. Any possible border search of letter class mail ("LC") shall be coordinated with CBP Officers assigned to such international mail facility and must conform to the guidelines set forth in CBP Handbook 3200-06A, International Mail Operations and Enforcement Handbook, or any successor document. Additionally, the U.S. Postal Service requires that it be notified and present at any border search of LC mail. Consultation with the ICE Office of Chief Counsel or the local U.S. Attorney's Office is recommended when considering a border search of any article that may be considered mail.
- b) Letters carried by individuals or private carriers such as DHL, UPS, or Federal Express, for example, are not considered to be mail, even if they are stamped, and thus are subject to border search as provided in this Directive. *See* 19 C.F.R. § 145.3.

### 3) Business Information.

If, in the course of a border search, ICE personnel encounter business or commercial information, ICE personnel shall treat such information 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.

### 4) Identification and travel documents.

Even without any suspicion of illegality, for legitimate, government purposes, ICE personnel may copy, retain, and share:

- (1) identification documents such as United States or foreign Passports, Certificates of Naturalization, Seaman's Papers, Airman Certificates, driver's licenses, state identification cards, and similar governmental identification documents, and

(2) travel documents that relate to the person's mode and date of travel into or out of the United States.

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 Julie L. Myers  
Julie L. Myers  
Assistant Secretary



## **PRIVACY THRESHOLD ANALYSIS (PTA)**

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	Click here to enter text.		
<b>Component:</b>	Choose an item.	<b>Office or Program:</b>	Click here to enter text.
<b>Xacta FISMA Name (if applicable):</b>	Click here to enter text.	<b>Xacta FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	Choose an item.	<b>Project or program status:</b>	Choose an item.
<b>Date first developed:</b>	Click here to enter a date.	<b>Pilot launch date:</b>	Click here to enter a date.
<b>Date of last PTA update</b>	Click here to enter a date.	<b>Pilot end date:</b>	Click here to enter a date.
<b>ATO Status (if applicable)</b>	Choose an item.	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

(b)(5)

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	Click here to enter text.		
<b>Office:</b>	Click here to enter text.	<b>Title:</b>	Click here to enter text.
<b>Phone:</b>	Click here to enter text.	<b>Email:</b>	Click here to enter text.

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	Click here to enter text.		
<b>Phone:</b>	Click here to enter text.	<b>Email:</b>	Click here to enter text.



(b)(5)

### SPECIFIC PTA QUESTIONS

<p><b>1. Reason for submitting the PTA: Choose an item.</b></p> <p><i>Please provide a general description of the project and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal please state whether or not there were any changes to the project, program, or system since the last {version}</i></p>
---

<p><b>2. Does this system employ any of the following technologies:</b></p> <p><i>If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.</i></p>	<input type="checkbox"/> Closed Circuit Television (CCTV) <input type="checkbox"/> Social Media <input type="checkbox"/> Web portal <sup>1</sup> (e.g., SharePoint) <input type="checkbox"/> Contact Lists <input type="checkbox"/> None of these
---	---

<p><b>3. From whom does the Project or Program collect, maintain, use, or disseminate information?</b></p> <p><i>Please check all that apply.</i></p>	<input type="checkbox"/> This program does not collect any personally identifiable information <sup>2</sup> <input type="checkbox"/> Members of the public <input type="checkbox"/> DHS employees/contractors (list components): <input type="checkbox"/> Contractors working on behalf of DHS <input type="checkbox"/> Employees of other federal agencies
---	---

<sup>1</sup> Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

<sup>2</sup> DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



<b>4. What specific information about individuals is collected, generated or retained?</b>	
<i>Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individuals.</i>	
<b>4(a) Does the project, program, or system retrieve information by personal identifier?</b>	<input type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If yes, please list all personal identifiers used:
<b>4(b) Does the project, program, or system use Social Security Numbers (SSN)?</b>	<input type="checkbox"/> No. <input type="checkbox"/> Yes.
<b>4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:</b>	Click here to enter text.
<b>4(d) If yes, please describe the uses of the SSNs within the project, program, or system:</b>	Click here to enter text.
<b>4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure?</b>  <i>For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?</i>	<input type="checkbox"/> No. Please continue to next question. <input type="checkbox"/> Yes. If a log kept of communication traffic, please answer the following question.
<b>4(f) If header or payload data<sup>3</sup> is stored in the communication traffic log, please detail the data elements stored.</b>	
Click here to enter text.	

<b>5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems<sup>4</sup>?</b>	<input type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list:  Click here to enter text.
--	---

<sup>3</sup> When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

<sup>4</sup> PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.



<p><b>6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?</b></p>	<p><input type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list:</p> <p>Click here to enter text.</p>
<p><b>6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?</b></p>	<p>Choose an item.</p> <p>Please describe applicable information sharing governance in place:</p>
<p><b>7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?</b></p>	<p><input type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. If yes, please list:</p>
<p><b>8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?</b></p>	<p><input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting:</p> <p><input type="checkbox"/> Yes. In what format is the accounting maintained:</p>
<p><b>9. Is there a FIPS 199 determination?<sup>4</sup></b></p>	<p><input type="checkbox"/> Unknown.</p> <p><input type="checkbox"/> No.</p> <p><input type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p>Confidentiality:  <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity:  <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Availability:  <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p>

<sup>4</sup> FIPS 199 is the [Federal Information Processing Standard](#) Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.



### PRIVACY THRESHOLD REVIEW

#### (TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

<b>Component Privacy Office Reviewer:</b>	Click here to enter text.
<b>Date submitted to Component Privacy Office:</b>	Click here to enter a date.
<b>Date submitted to DHS Privacy Office:</b>	Click here to enter a date.
<b>Component Privacy Office Recommendation:</b> <i>Please include recommendation below, including what new privacy compliance documentation is needed.</i>	
Click here to enter text.	

#### (TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

<b>DHS Privacy Office Reviewer:</b>	Click here to enter text.
<b>PCTS Workflow Number:</b>	Click here to enter text.
<b>Date approved by DHS Privacy Office:</b>	Click here to enter a date.
<b>PTA Expiration Date</b>	Click here to enter a date.

### DESIGNATION

<b>Privacy Sensitive System:</b>	Choose an item. If "no" PTA adjudication is complete.
<b>Category of System:</b>	Choose an item. If "other" is selected, please describe: Click here to enter text.
<b>Determination:</b>	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. <input type="checkbox"/> Privacy Act Statement required. <input type="checkbox"/> Privacy Impact Assessment (PIA) required. <input type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Paperwork Reduction Act (PRA) Clearance may be required. Contact



<p>your component PRA Officer.</p> <p><input type="checkbox"/> A Records Schedule may be required. Contact your component Records Officer.</p>	
<b>PIA:</b>	<p>Choose an item.</p> <p>If covered by existing PIA, please list: <a href="#">Click here to enter text.</a></p>
<b>SORN:</b>	<p>Choose an item.</p> <p>If covered by existing SORN, please list: <a href="#">Click here to enter text.</a></p>
<p><b>DHS Privacy Office Comments:</b> <i>Please describe rationale for privacy compliance determination above.</i></p>	
<p><a href="#">Click here to enter text.</a></p>	



## **PRIVACY THRESHOLD ANALYSIS (PTA)**

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.

Page 747

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 748

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 749

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 750

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 751

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 752

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 753

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act



## **PRIVACY THRESHOLD ANALYSIS (PTA)**

**This form is used to determine whether a Privacy Impact Assessment is required.**

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance  
The Privacy Office  
U.S. Department of Homeland Security  
Washington, DC 20528  
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), on DHSCconnect and directly from the DHS Privacy Office via email: [pia@hq.dhs.gov](mailto:pia@hq.dhs.gov), phone: 202-343-1717.



(b)(5)

## PRIVACY THRESHOLD ANALYSIS (PTA)

### SUMMARY INFORMATION

<b>Project or Program Name:</b>	HSI Cell Site Simulator Log SharePoint Site		
<b>Component:</b>	Immigration and Customs Enforcement (ICE)	<b>Office or Program:</b>	Homeland Security Investigations (HSI) Technical Operations Unit (TechOps)
<b>Xacta FISMA Name (if applicable):</b>	Click here to enter text.	<b>Xacta FISMA Number (if applicable):</b>	Click here to enter text.
<b>Type of Project or Program:</b>	IT System	<b>Project or program status:</b>	Development
<b>Date first developed:</b>	(b)(5)	<b>Pilot launch date:</b>	Click here to enter a date.
<b>Date of last PTA update</b>	Click here to enter a date.	<b>Pilot end date:</b>	Click here to enter a date.
<b>ATO Status (if applicable)</b>	Choose an item.	<b>ATO expiration date (if applicable):</b>	Click here to enter a date.

### PROJECT OR PROGRAM MANAGER

<b>Name:</b>	Keith Kelly		
<b>Office:</b>	HSI TechOps	<b>Title:</b>	National Program Manager, Technical Enforcement Officer
<b>Phone:</b>	(703) 551-5521	<b>Email:</b>	Keith.Kelly@ice.dhs.gov

### INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

<b>Name:</b>	Click here to enter text.		
<b>Phone:</b>	Click here to enter text.	<b>Email:</b>	Click here to enter text.

Page 756

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 757

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 758

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 759

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 760

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 761

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 762

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 763

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 764

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 765

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 766

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 767

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 768

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 769

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 770

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 771

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 772

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 773

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 774

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 775

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 776

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 777

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 778

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 779

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 780

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 781

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 782

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 783

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 764

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 785

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 786

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 787

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 788

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 789

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 790

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 791

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 792

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 793

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 794

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 795

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 796

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 797

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 798

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 799

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 800

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 801

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 802

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 803

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 804

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 805

Withheld pursuant to exemption

(b)(5); WIF Draft

of the Freedom of Information and Privacy Act

Page 806

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 807

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 808

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act