

Page 126

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 127

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 128

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 129

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 130

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 131

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 132

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 133

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 134

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 135

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 136

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 137

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 138

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Page 139

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 140

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 141

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 142

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 143

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 144

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 145

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 146

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 147

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 146

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 149

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 150

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 151

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 152

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 153

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 154

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 155

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 156

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 157

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 158

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 159

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 160

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 161

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 162

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 163

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 164

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 165

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 166

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 167

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 168

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

U.S. CUSTOMS AND BORDER PROTECTION

CBP DIRECTIVE NO. 3340-049

DATE: August 20, 2009

ORIGINATING OFFICE: FO:TO

SUPERSEDES:

REVIEW DATE: August 2012

SUBJECT: BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION

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

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

2 POLICY.

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

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

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

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

CBP Form 232C (04/03)

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

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

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

3 DEFINITIONS.

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

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

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

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

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

5 PROCEDURES.

5.1 Border Searches.

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

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

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

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

5.2 Review and Handling of Privileged or Other Sensitive Material.

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

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

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

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

5.3 Detention and Review in Continuation of Border Search of Information

5.3.1 Detention and Review by CBP

An Officer may detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search. The search may take place on-site or at an off-site location, and is to be completed as expeditiously as possible. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) days.

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

5.3.1.2 Destruction. Except as noted in section 5.4 or elsewhere in this Directive, if after reviewing the information pursuant to the time frames discussed in section 5.3, there is not probable cause to seize it, any copies of the information must be destroyed, and any electronic device must be returned. Upon this determination that there is no value to the information copied from the device, the copy of the information is destroyed as expeditiously as possible, but no later than seven (7) days after such determination unless circumstances require additional time, which must be approved by a supervisor and documented in an appropriate CBP system of records and which must be no later than twenty one (21) days after such determination. The destruction shall be noted in appropriate CBP systems of records.

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

law enforcement or other operational considerations, the individual may be notified of the purpose and authority for these types of searches, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search.

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

5.3.2 Assistance by Other Federal Agencies.

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

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

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

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

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

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

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

5.3.3 Responses and Time for Assistance

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

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

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

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

5.4 Retention and Sharing of Information Found in Border Searches

5.4.1 Retention and Sharing of Information Found in Border Searches

5.4.1.1 Retention with Probable Cause. Officers may seize and retain an electronic device, or copies of information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents thereof, contains evidence of or is the fruit of a crime that CBP is authorized to enforce.

5.4.1.2 Retention of Information in CBP Privacy Act-Compliant Systems. Without probable cause to seize an electronic device or a copy of information contained therein, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. For example, information collected in the course of immigration processing for the purposes of present and future admissibility of an alien may be retained in the A-file, Central Index System, TECS, and/or ENFORCE or other systems as may be appropriate and consistent with the policies governing such systems.

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

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

5.4.1.5 Safeguarding Data During Storage and Transmission. CBP will appropriately safeguard information retained, copied, or seized under this Directive and during transmission to another federal agency. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking copies to ensure appropriate disposition, and other safeguards during transmission such as password

protection or physical protections. Any suspected loss or compromise of information that contains personal data retained, copied, or seized under this Directive must be immediately reported to the Port Director, Patrol Agent in Charge or equivalent level manager and the CBP Office of Internal Affairs.

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

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

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

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

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

5.5 Reporting Requirements

5.5.1 The Officer performing the border search of information shall be responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Form 6051D when appropriate, and creation and/or updating records in CBP systems. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition including supervisory approvals and extensions when appropriate.

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

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

5.6 Management Requirements

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

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

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

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

6 MEASUREMENT. CBP Headquarters will continue to develop and maintain appropriate mechanisms to ensure that statistics regarding border searches of electronic devices, and the results thereof, can be generated from CBP systems using data elements entered by Officers pursuant to this Directive.

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

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

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

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


Acting Commissioner
U.S. Customs and Border Protection



Attachment 2

ICE Directive

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
ICE Policy System

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

DIRECTIVE TITLE: BORDER SEARCHES OF ELECTRONIC DEVICES

1. PURPOSE and SCOPE.

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

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

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

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

Border Searches of Electronic Devices

- 4. BACKGROUND.** ICE is responsible for ensuring compliance with customs, immigration, and other Federal laws at the border. To that end, Special Agents may review and analyze computers, disks, hard drives, and other electronic or digital storage devices. These searches are part of ICE's long-standing practice and are essential to enforcing the law at the United States border. Searches of electronic devices are a crucial tool for detecting information concerning terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws.
- 5. DEFINITIONS.** The following definitions are provided for the purposes of this Directive:
- 5.1. Assistance.** The use of third party analytic resources such as language processing, decryption, and subject matter expertise, to assist ICE in viewing the information contained in electronic devices or in determining the meaning, context, or value of information contained therein.
- 5.2. Electronic Devices.** Any item that may contain information, such as computers, disks, drives, tapes, mobile phones and other communication devices, cameras, music players, and any other electronic or digital devices.
- 6. POLICY.**
- 6.1.** ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth herein. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate.
- 6.2.** When U.S. Customs and Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE.
- 6.3.** Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic recordkeeping systems.
- 7. RESPONSIBILITIES.**
- 7.1.** The Directors of OI, the Office of Professional Responsibility (OPR), and the Office of International Affairs (OIA) have oversight over the implementation of the provisions of this Directive.
- 7.2.** Special Agents in Charge (SACs) and Attachés are responsible for:

- 1) Implementing the provisions of this Directive and ensuring that Special Agents in their area of responsibility (AOR) receive a copy of this Directive and are familiar with its contents;
- 2) Ensuring that Special Agents in their AOR have completed any training programs relevant to border searches of electronic devices, including constitutional, privacy, civil rights, and civil liberties training related to such searches, as may be required by ICE Headquarters; and
- 3) Maintaining appropriate mechanisms for internal audit and review of compliance with the procedures outlined in this Directive. (See "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Devices" memo dated December 12, 2008.)

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

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

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

8. PROCEDURES.

8.1. Border Searches by ICE Special Agents.

- 1) Authorization to Conduct Border Search. Border searches of electronic devices must be performed by an ICE Special Agent who meets the definition of "customs officer" under 19 U.S.C. § 1401(i), or another properly authorized officer with border search authority, such as a CBP Officer or Border Patrol Agent, persons cross designated by ICE as customs officers, and persons whose assistance to ICE is demanded under 19 U.S.C. § 507.
- 2) Knowledge and Presence of the Traveler. To the extent practicable, border searches should be conducted in the presence of, or with the knowledge of, the traveler. When not practicable due to law enforcement, national security, or other operational concerns, such circumstances are to be noted by the Special Agent in appropriate ICE systems. Permitting an individual to be present in the room during a search does not necessarily mean that the individual will be permitted to witness the search itself. If permitting an individual to witness the search itself could reveal law enforcement

Border Searches of Electronic Devices

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

- 3) Consent Not Needed. At no point during a border search of electronic devices is it necessary to ask the traveler for consent to search.
- 4) Continuation of the Border Search. At any point during a border search, electronic devices, or copies of information therefrom, may be detained for further review either on-site at the place of detention or at an off-site location, including a location associated with a demand for assistance from an outside agency or entity (see Section 8.4).
- 5) Originals. In the event electronic devices are detained, the Special Agent should consider whether it is appropriate to copy the information therefrom and return the device. When appropriate, given the facts and circumstances of the matter, any such device should be returned to the traveler as soon as practicable. Consultation with the Office of the Chief Counsel is recommended when determining whether to retain a device in an administrative immigration proceeding. Devices will be returned to the traveler as expeditiously as possible at the conclusion of a negative border search.

8.2. Chain of Custody.

- 1) Detentions of electronic devices. Whenever ICE detains electronic devices, or copies of information therefrom, the Special Agent will initiate the correct chain of custody form or other appropriate documentation.
- 2) Seizures of electronic devices for criminal purposes. Whenever ICE seizes electronic devices, or copies of information therefrom, the Special Agent is to enter the seizure into the appropriate ICE systems. Additionally, the seizing agent must complete the correct chain of custody form or other appropriate documentation.
- 3) Retention of electronic devices for administrative immigration purposes. Whenever ICE retains electronic devices, or copies of information therefrom, or portions thereof, for administrative immigration purposes pursuant to 8 U.S.C. § 1357, the Special Agent is to record such retention in appropriate ICE systems and is to include the location of the retained files, a summary thereof, and the purpose for retention.
- 4) Notice to traveler. Whenever ICE detains, seizes, or retains original electronic devices, the Special Agent is to provide the traveler with a copy of the applicable chain of custody form or other appropriate documentation.

8.3. Duration of Border Search.

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

Border Searches of Electronic Devices

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

- 2) Special Agents seeking assistance from other Federal agencies or non-Federal entities are responsible for ensuring that the results of the assistance are received in a reasonable time (see Section 8.4(5)).
- 3) In determining “reasonable time,” courts have reviewed the elapsed time between the detention and the completion of the border search, taking into account any additional facts and circumstances unique to the case. As such, ICE Special Agents are to document the progress of their searches, for devices and copies of information therefrom, and should consider the following factors:
 - a) The amount of information needing review;
 - b) Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;
 - c) Whether assistance was sought and the type of such assistance;
 - d) Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;
 - e) Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and
 - f) Any unanticipated exigency that may arise.

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

- 1) Translation, Decryption, and Other Technical Assistance.
 - a) During a border search, Special Agents may encounter information in electronic devices that presents technical difficulties, is in a foreign language, and/or encrypted. To assist ICE in conducting a border search or in determining the meaning of such information, Special Agents may demand translation, decryption, and/or technical assistance from other Federal agencies or non-Federal entities.
 - b) Special Agents may demand such assistance absent individualized suspicion.
 - c) Special Agents shall document such demands in appropriate ICE systems.

2) Subject Matter Assistance.

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

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

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

5) Time for Assistance and Responses Required.

- a) Assistance is to be accomplished within a reasonable period of time in order to preserve the status of the electronic devices and the integrity of the border search.
- b) It is the responsibility of the Special Agent demanding the assistance to ensure timely responses from assisting agencies or entities and to act in accord with section 8.3 of this Directive. In addition, Special Agents shall:
 - i) Inform assisting agencies or entities that they are to provide results of assistance as expeditiously as possible;
 - ii) Ensure that assisting agencies and entities are aware that responses to ICE must include any findings, observations, and conclusions drawn from their review that may relate to the laws enforced by ICE;

- iii) Contact the assisting agency or entity to get a status report on the demand within the first 30 calendar days;
- iv) Remain in communication with the assisting agency or entity until results are received;
- v) Document all communications and actions in appropriate ICE systems; and
- vi) Consult with a supervisor to determine appropriate action if the timeliness of results is a concern. If a demand for assistance is revoked, the Special Agent is to ensure all electronic devices are returned to ICE as expeditiously as possible.

8.5. Retention, Sharing, Safeguarding, And Destruction.

1) By ICE

- a) Seizure and Retention with Probable Cause. When Special Agents determine there is probable cause of unlawful activity—based on a review of information in electronic devices or on other facts and circumstances—they may seize and retain the electronic device or copies of information therefrom, or relevant portions thereof, as authorized by law.
- b) Retention of Information in ICE Systems. To the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. For example, information entered into TECS during the course of an investigation will be retained consistent with the policies governing TECS.
- c) Sharing. Copies of information from electronic devices, or portions thereof, which are retained in accordance with this section, may be shared by ICE with Federal, state, local, and foreign law enforcement agencies in accordance with applicable law and policy. Sharing must be in compliance with the Privacy Act and applicable ICE privacy policies, such as the ICE Search, Arrest, and Seizure System of Records Notice.
- d) Safeguarding Data During Storage and Transmission. ICE will appropriately safeguard information detained, copied, retained, or seized under this directive while in ICE custody and during transmission to an outside entity. Appropriate safeguards include keeping materials in locked cabinets or rooms, documenting and tracking originals and copies to ensure appropriate disposition, and appropriate safeguards during transmission such as encryption of electronic data or physical protections (e.g., locked containers). Any suspected loss or compromise of information that contains personal data detained, copied, or seized under this directive must be reported immediately to the ICE Service Desk.

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

2) By Assisting Agencies

- a) Retention during Assistance. All electronic devices, whether originals or copies of information therefrom, provided to an assisting Federal agency may be retained by that agency for the period of time needed to provide the requested assistance to ICE.
- b) Return or Destruction. At the conclusion of the requested assistance, all electronic devices and data must be returned to ICE as expeditiously as possible. In the alternative, the assisting Federal agency may certify to ICE that any copies in its possession have been destroyed or it may advise ICE in accordance with Section 8.5(2)(c). In the event that any original electronic devices were transmitted, they must not be destroyed; they are to be returned to ICE.
- c) Retention with Independent Authority. Copies may be retained by an assisting Federal agency only if and to the extent that it has the independent legal authority to do so – for example, when the information is of national security or intelligence value. In such cases, the retaining agency must advise ICE of its decision to retain certain information on its own authority. In the event that any original electronic devices were transmitted, the assisting Federal agency may make a copy of information therefrom for its retention; however, any originals must be returned to ICE.

3) By Non-Federal Entities

- a) ICE may provide copies of information from electronic devices to an assisting non-Federal entity, such as a private language translation or data decryption service, only for the period of time needed by that entity to render the requested assistance.
- b) Upon the completion of assistance, all copies of the information in the possession of the entity must be returned to ICE as expeditiously as possible. Any latent copies of the electronic data on the systems of the non-Federal entity must also be destroyed so that recovery of the data is impractical.

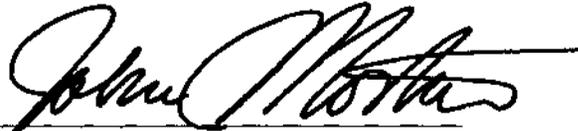
8.6. Review, Handling, and Sharing of Certain Types of Information.

- 1) Border Search. All electronic devices crossing U.S. borders are subject to border search; a claim of privilege or personal information does not prevent the search of a traveler's information at the border. However, the nature of certain types of information are subject to special handling by Special Agents, whether through policy or laws such as the Privacy Act and the Trade Secrets Act.
- 2) Types of Information
 - a) Business or Commercial Information. If, in the course of a border search, Special Agents encounter business or commercial information, such information is to be treated as business confidential information. Depending on the nature of the information presented, the Trade Secrets Act, the Privacy Act, and other laws may specifically govern or restrict handling of the information, including criminal penalties for unauthorized disclosure.
 - b) Legal Information. Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems.
 - c) Other Sensitive Information. Other possibly sensitive information, such as medical records and work-related information carried by journalists shall be handled in accordance with all applicable federal law and ICE policy. Although there is no Federal legal privilege pertaining to the doctor-patient relationship, the inherent nature of medical information warrants special care for such records. Questions regarding the review of these materials shall be directed to the ICE Office of the Chief Counsel and this consultation shall be noted in appropriate ICE systems.
- 3) Sharing. Information that is determined to be protected by law as privileged or sensitive is to be handled consistent with the laws and policies governing such information.

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

- 8.8 Audit.** ICE Headquarters will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive.
- 9. ATTACHMENTS.** None.
- 10. NO PRIVATE RIGHT STATEMENT.** This Directive is an internal policy statement of ICE. It is not intended to, and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees; or any other person.

Approved



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

Page 190

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 191

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 192

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 193

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 194

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 195

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 196

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 197

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 198

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 199

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 200

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 201

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

Page 202

Withheld pursuant to exemption

(b)(5);WIF Draft

of the Freedom of Information and Privacy Act

From: (b)(6);(b)(7)(C)
Sent: 12 Jan 2018 12:52:11 -0500
To: (b)(6);(b)(7)(C)
Cc:
Subject: RE: ICE Use of Cellebrite Technology
Attachments: dhs-pta-template.dotx

(b)(6);(b)(7)(C)

Do either of you know if something similar was done for Cellebrite already? I think the initial IDIQ was done in 2013 (which means we need a new one done this year) and I know I have seen some Privacy documents for Cellebrite when we exercise the options. Just not sure where those are located. The only reference to a PTA I found on the shared drive was for NUIX.

Special Agent (b)(6);(b)(7)(C)
Computer Forensics Unit
U.S. Department of Homeland Security
ICE/HSI Cyber Crimes Center (C3)
11320 Random Hills Rd., Suite (b)(6);(b)(7)(C)
Fairfax, VA 22030 (U.S. Postal - 20598)
Phone: 703-293-(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

From: (b)(6);(b)(7)(C)
Sent: Friday, January 12, 2018 11:44 AM
To: (b)(6);(b)(7)(C)
Cc:
Subject: FW: ICE Use of Cellebrite Technology

Hi (b)(6);(b)(7)(C)

Yesterday, Privacy approved a procurement for renewal licenses for EXBS Jordan Cellebrite.

(b)(5)
(b)(5) We would like to complete a Privacy Threshold Analysis (PTA) for our use of this technology. A PTA is an internal document that allows us to record privacy compliance coverage for a system or technology. PTAs are reviewed only by ICE Privacy and the DHS HQ Privacy Office, and unlike Privacy Impact Assessments, are not published.

I have attached the PTA template here, which we would greatly appreciate your/your staff's help completing

Of course, I am always happy to chat about your questions or concerns.

(b)(6);(b)(7)(C)
Privacy Compliance Specialist
Privacy Branch
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement

Main: (202) 732-(b)(6)
Direct: (202) 732-(b)(6)
Mobile: (202) 878-(b)(6)

Questions? Please visit the Office of Information Governance & Privacy website at <https://insight.ice.dhs.gov/mgt/oop/Pages/index.aspx>.



U.S. Immigration
and Customs
Enforcement

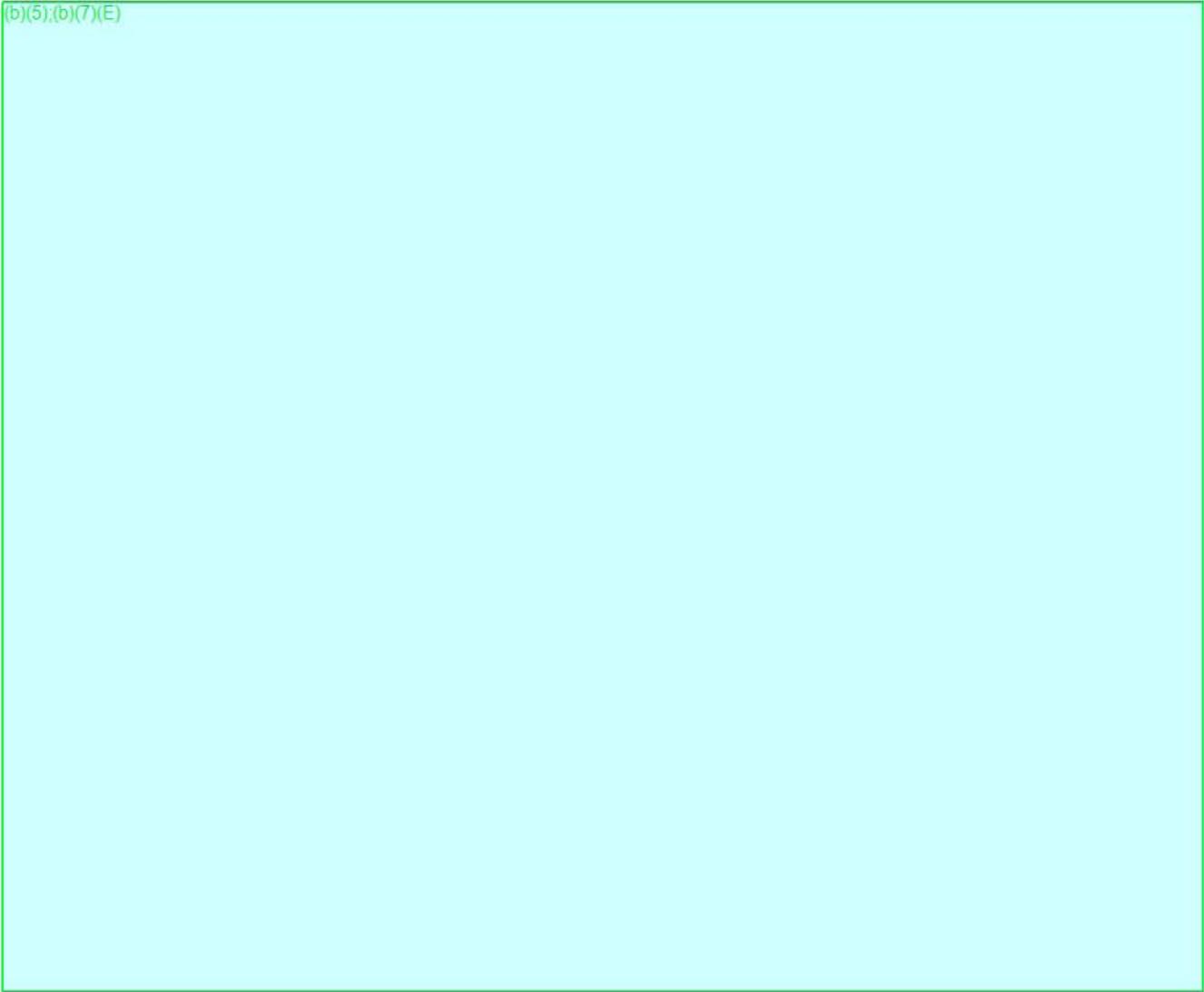
ICE Mobile Applications Development Approvals/Governance Process

Light, Lean, Fast, Action, and Results!

Final Document
Version 6 as of 2013-09-06

Contents

(b)(5);(b)(7)(E)



Page 207

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 208

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 209

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 210

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 211

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 212

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 213

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 214

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 215

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

(b)(5),(b)(7)(E)

Points of Contact for Assistance:

(b)(6),(b)(7)(C)

ICE Mobility Program Manager	202-732-	(b)(6),(b)(7)(C)
Mobile Applications Project Manager	202-732-	(b)(6),(b)(7)(C)
Architecture/ Section 508/SLM	202-732-	(b)(6),(b)(7)(C)
Technical Architecture	202-732-	(b)(6),(b)(7)(C)
Information Assurance	202-732-	(b)(6),(b)(7)(C)
CAE / Governance	202-732-	(b)(6),(b)(7)(C)

Page 217

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 218

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 219

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 220

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 221

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 222

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 223

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 224

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 225

Withheld pursuant to exemption

(b)(5);(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 226

Withheld pursuant to exemption

(b)(6);(b)(7)(C)

of the Freedom of Information and Privacy Act

Page 227

Withheld pursuant to exemption

WIF Draft;(b)(5)

of the Freedom of Information and Privacy Act

Study: Cloud Service Agreements Omit Key Considerations

New ISO/IEC 19086-1 Standard Guides Organizations To Structured, Effective Agreements

Table Of Contents

Executive Summary	2
There's More To Cloud Service Provider Selection Than Cost	2
Cloud Agreements Are Often Missing Key Considerations	3
Key Recommendations	8
Appendix A: Methodology	9
Appendix B: Supplemental Material	9
Appendix C: Endnotes.....	9

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2016, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [1-TWE210]

Project Director: N(b)(6);(b)(7) Senior Consultant, Market Impact Consulting
 Contributing Research: Forrester's Sourcing And Vendor Management Research Group

Executive Summary

In an era where organizations require more agility than ever to keep up with changing demands of technologically empowered customers, cloud computing has become a compelling method for reaching new markets faster and staying ahead of the competition.¹ As organizations build out complex cloud ecosystems with multiple cloud service providers (CSPs), they often struggle with contracting and governance — issues that begin with highly variable cloud procurement agreements that are in place across various cloud service providers.

Recognizing this challenge, the International Organization for Standardization (ISO), an international standard-setting body that develops worldwide technological and manufacturing standards, is establishing a standard for cloud compliance agreements and SLA frameworks and technology. This standard, the ISO/IEC 19086-1 Standard², offers some much needed structure and guidance to cloud contracts that will help inform CSPs and buyers alike.

In June 2016, Microsoft commissioned Forrester Consulting to evaluate the current state of cloud agreements against the elements of the forthcoming standard. To further explore this trend, Forrester tested the hypothesis that many organizations are overlooking service-level and service-quality objectives in their RFPs and cloud service agreements.

Ninety-four percent of respondents would have changed something about their most recent cloud agreement.

In conducting an online survey of 467 enterprises, small and medium-size businesses (SMBs), and government organizations, Forrester found that organizations lack standardization in their cloud agreements and often omit considerations that are important to their evolving organizations.

KEY FINDINGS

Forrester's study yielded three key findings:

- › **There's more to cloud service provider selection than cost.** In an era where business agility is paramount to win, serve, and retain customers, organizations are expanding their use of the cloud. With emerging cloud technology, the demands for new skills and expertise are increasingly required, and many organizations must turn to managed service providers to help them transform their existing services into fully cloud-based equivalents. In turn, businesses have high demands from their CSPs. Rather than solely prioritizing costs in their CSP selection process, they prefer CSPs that can lend their business process expertise to help fulfill growing needs for innovation and improving the business technology (BT) agenda.³
- › **Cloud agreements are often missing key considerations.** The unique and complex nature of the cloud means that many common IT services contract stipulations may not be relevant. Customers often push for very stringent SLAs and penalties and, in turn, the CSPs push back. The result is customized and highly variable cloud agreements that lead to some level of buyers' remorse, as businesses suffer the consequences of narrowly focused agreements.
- › **The ISO/IEC 19086-1 Standard will help organizations meet new requirements.** Evolving business demands will continue to add complexity to the cloud procurement process. Most organizations use some form of external guidance to help them navigate this complexity and ensure that they are including the considerations that are of highest priority to them; however, most existing external guidance documents are not comprehensive, and organizations admit to missing key considerations. The ISO standard will provide much-needed definitions and a checklist of key information that cloud buyers can use to help ensure that they haven't overlooked any considerations in negotiating cloud agreements.

There's More To Cloud Service Provider Selection Than Cost

Cloud technologies are widely praised for their agility, scalability, and subscription-based agreements that require fewer upfront capital expenditures. As decision-makers gain comfort with the cloud, they are adopting it in increasingly larger deployments covering more technology areas and mission-critical tasks. As the adoption of cloud increases, so do the associated costs and risks, making it critical for procurement professionals to pay extra care in drafting the right agreements with the right CSPs. Our study found that:

- › **Most respondents have multiple cloud service model deployments.** Our study surveyed respondents who have deployed at least one cloud service, but we found that most are deploying multiple types of cloud services. The most prevalent is software-as-a-service (SaaS), which is deployed by 78% of respondents, followed by platform-as-a-service (PaaS) (64%) and infrastructure-as-a-service (IaaS) (61%) (see Figure 1).
- › **Business continuity, improved IT infrastructure flexibility, security, and compliance are key drivers of cloud adoption.** There is a wide range of considerations that factor into the decision to adopt cloud. Our study found 13 separate considerations that respondents all ranked as “important” or “very important” drivers. These considerations fell into a few major categories — namely flexibility and agility, on-demand scalability, easier management, and better disaster recovery/compliance. The lattermost category is of particular importance when companies are choosing CSPs, as security, privacy, and compliance concerns are traditionally considered barriers to cloud adoption, and costs associated with breaches and/or noncompliance can be quite high.⁴
- › **A significant proportion of overall IT management is provided by cloud service providers.** Technology management teams often need help with choosing the right solutions for various workloads and transferring their services into the cloud; therefore, they turn to their cloud providers as partners.⁵ IT departments frequently rely on CSPs — as well as other third-party service providers — to manage their applications (55%), but they also rely on them for other areas of their infrastructure such as platform architecture (47%), virtualized infrastructure (46%), facility (44%), and hardware (43%). Responsibility for these components is quite variable across cloud

FIGURE 1
Organizations Commonly Use Multiple Cloud Services

“Which of the following types of cloud services has your organization deployed?”



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

agreements, as roughly 40% of organizations self-manage each of these on average. Organizations are more likely to self-manage IaaS deployments and least likely to self-manage SaaS deployments.

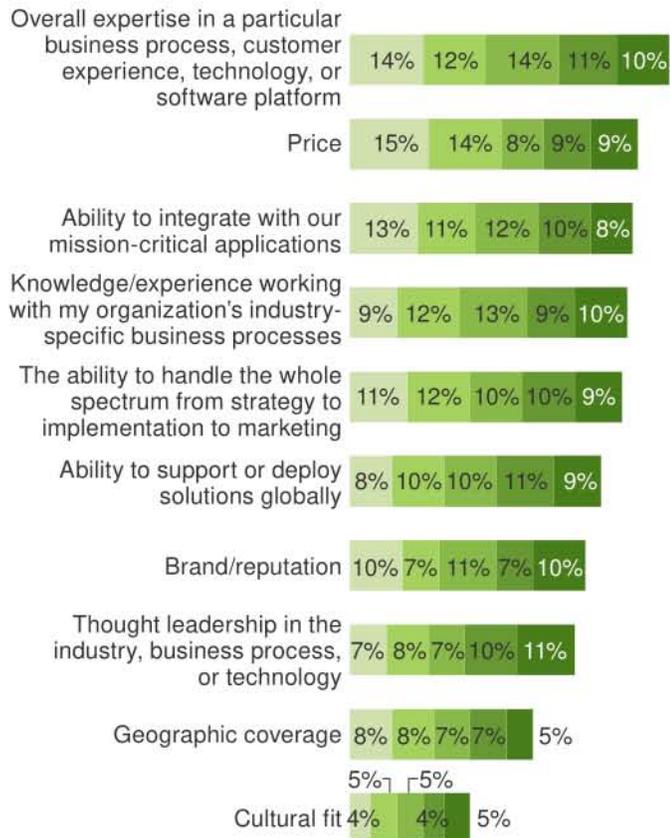
- › **Expertise is the top criterion for selecting a cloud service provider.** Price is always an important consideration for CSP selection (and is the second-highest-ranked criterion by decision-makers), but there are many other important factors when selecting a CSP. Many organizations are involving CSPs that offer business process or vertical capabilities in addition to core cloud services. The number one factor is overall expertise — whether in a particular business process, customer experience, technology, or software platform. This was ranked as a top-five criterion by 61% of respondents. Other important factors include the ability to integrate with mission-critical applications, industry-specific knowledge, soup-to-nuts capabilities from implementation to marketing, and the ability to deploy and support global implementations (see Figure 2).

FIGURE 2

Buyers Look For Cloud Service Providers That Support Their Business Technology Agenda

“Which of the following criteria are most important to your organization when selecting a service provider for a cloud implementation? Rank up to your top five.”

Rank 1 Rank 2 Rank 3 Rank 4 Rank 5



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

Cloud Agreements Are Often Missing Key Considerations

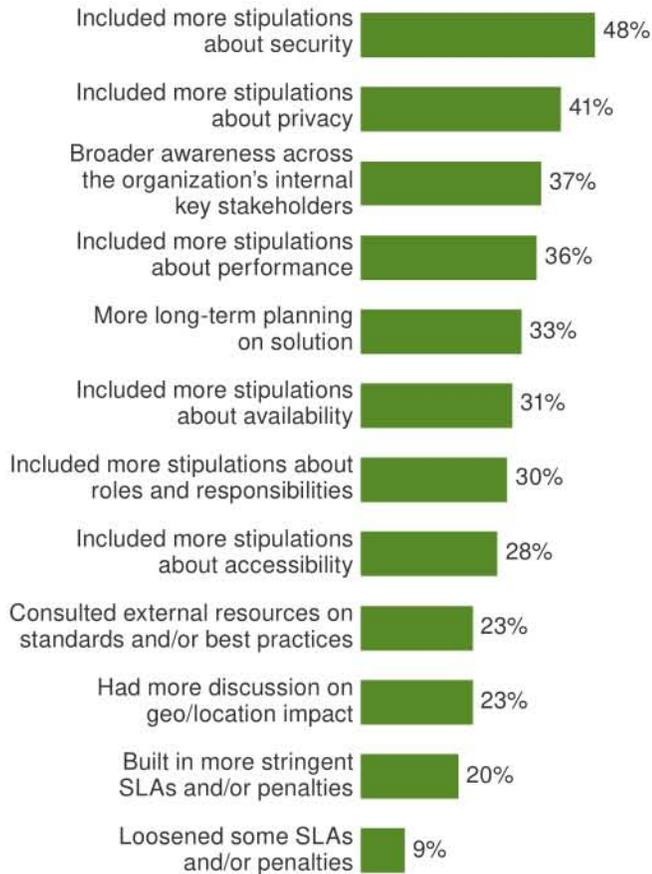
To better assess the value of the ISO standard (and similar checklists) to businesses, we asked cloud agreement decision-makers a series of questions regarding their most recent cloud deployments to understand what is working well for them and what they would like to have done differently in hindsight. While respondents are not wholly dissatisfied with their cloud agreements, we found that 57% were less than “very satisfied,” and even these respondents saw room for improvement. In our gap analysis, we uncovered the following insights:

- Ninety-four percent of respondents would have changed something about their most recent cloud agreement.** Due to their complex nature, cloud agreements almost invariably omit some considerations and SLAs, leading to consequences for the business when problems later arise. For example, 48% of respondents indicated that if they could redo their most recent cloud agreement, they would include more stipulations about security. Many respondents also would have included more stipulations about privacy (41%), performance (36%), availability (31%), roles and responsibilities (30%), and accessibility (28%). Cloud decision-makers also wish that they had incorporated more points of view and considerations when developing their cloud agreements, both from the organization's internal key stakeholders (37%) and from external resources on standards and best practices (23%) (see Figure 3). The procurement, risk management, and legal respondents we surveyed were the least satisfied with their most recent cloud agreements, indicating that perhaps they are not being involved heavily enough in the early stages of developing the agreements.

FIGURE 3

Cloud Buyers Would Like Cloud Agreements To Carry More Stipulations Around Security, Privacy, And Performance, Among Others

“Thinking about your most recent cloud agreement, what would you like to have done differently?”



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

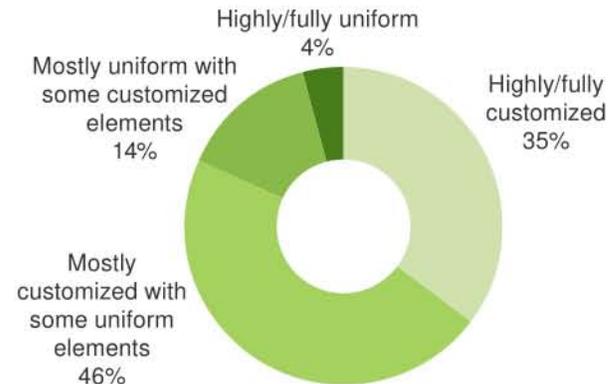
› **Cloud agreements tend to be highly customized, which is time consuming and leaves room for error.**

The fact that many agreements are missing critical stipulations is likely a byproduct of the fact that cloud agreements do not follow a consistent structure. Thirty-five percent of respondents reported that their cloud agreements are highly or fully customized, and another 46% indicated that their cloud agreements are mostly customized with some uniform elements. A mere 4% described their cloud agreements as highly/fully uniform (see Figure 4). Much of this heightened variability is due

FIGURE 4

Cloud Agreements Are Usually Customized

“Which of the following best describes the customization and uniformity of your cloud agreements?”



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

(Percentages may not total 100 because of rounding)

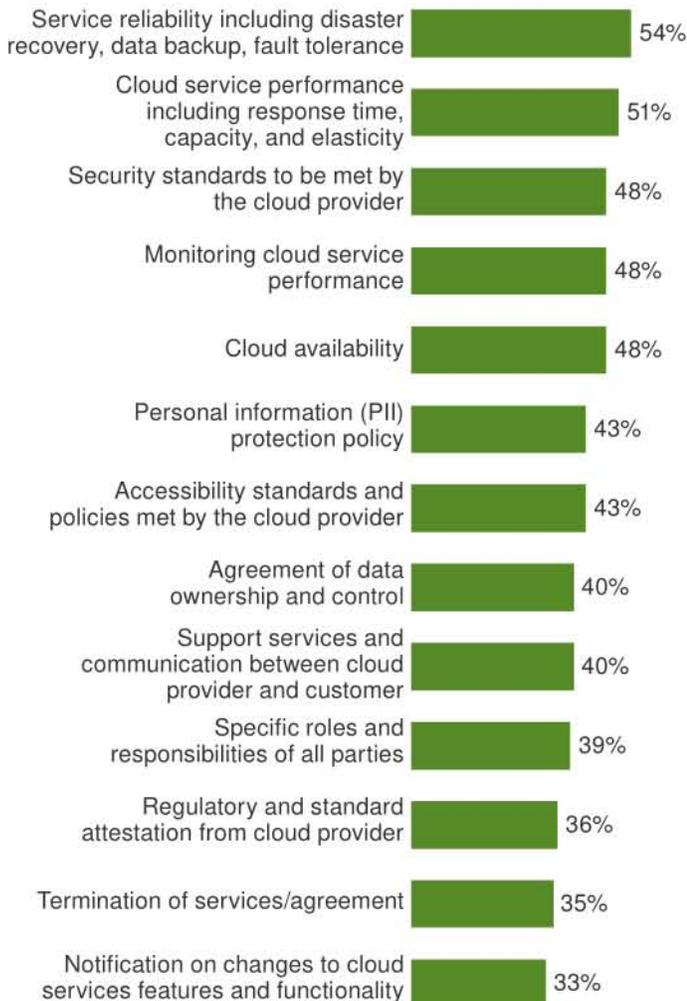
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

to CSPs' insistence on their own standardized agreements. While suppliers understandably seek to maintain control over agreements in order to deliver consistent services and stable environments, their agreement terms may not be aligned with the customers' own views of best practices and may leave IT professionals with significant responsibility for self-managing at least some elements of their cloud environments.⁶

- › **Components of the ISO standard are frequently omitted from cloud agreements.** We asked respondents to look over a list of criteria included in the ISO standard and found that many elements were not included in their most recent cloud agreements. The most frequently omitted components of a cloud agreement were notifications on changes to cloud service features and functionality (included only 33% of the time), language around termination of services (35%), and regulatory and standard attestations from cloud providers (33%). Even the most frequently included stipulations are only accounted for about half the time: 54% of agreements had service reliability stipulations including disaster recovery, data backup, and fault tolerance, and 51% had cloud service performance stipulations including response time, capacity, and elasticity (see Figure 5).

FIGURE 5
Most Agreements Omit Key “Best Practice” Considerations

“Thinking back to your most recent cloud agreement, which considerations were included?”



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

› **Non-optimized agreements lead to consequences.**

Missing terms are far from inconsequential; in fact, they can significantly hurt the organization. Consequences include delays in project delivery, a lack of quality control, and loss of profitability, among others. Eighty-nine percent of the respondents we surveyed have had at least one issue with a cloud service agreement that has carried some form of consequence.

The ISO/IEC 19086-1 Standard Will Help Organizations Meet New Requirements

The combination of evolving business demands along with the unique nature of the cloud continues to pose special challenges for customers who need to decide which of their typical IT services agreement considerations are relevant to cloud services (and worth fighting for when CSPs omit them). The emergence of published industry standards will help both CSPs and buyers by driving some homogeneity of terms over time in an industry that currently has significant agreement variability from CSP to CSP. For now, decision-makers can use the standard to ensure that they are negotiating the best practices for agreements and reducing risk for their organizations. Our study found that:

› **Most cloud agreement decision-makers use external standards/research and find them useful.** The majority of the decision-makers we surveyed consulted some form of external guidance when negotiating and/or setting criteria for their most recent cloud agreements. The most common tools are published standards and research from analyst firms, followed by conferences/events and blogs. These decision-makers find these tools to be quite useful as well: 98% of organizations that used research from analyst firms or published standards found them to be at least somewhat useful, and information gleaned from conferences and blogs was also seen as instrumental in guiding agreements. Only 6% of our respondents did not use any external guidance whatsoever, and 81% of those respondents indicated that such guidance would have been helpful. Despite their use of standards, many organizations still have issues with their cloud agreements. The ISO standard should provide a more robust checklist for organizations to ensure that they are no longer omitting important considerations.

› **Increased requirements and shifting priorities have a large impact on the structure and components of cloud agreements.** Digital technologies are evolving rapidly and are increasingly key components of organizations' strategies for winning, serving, and retaining customers. As new trends emerge, cloud agreements will need new considerations to reflect increased expectations. Our study found that the structure and components of recent cloud agreements have been affected by a number of evolving trends, including increasing demands for customization flexibility, self-service capabilities, automation, consulting-like service

offerings, and agile and continuous delivery practices (see Figure 6).

FIGURE 6
New Business Demands Lead To Shifting Requirements For Cloud Agreements

“Which of the following criteria are most important to your organization when selecting a service provider for a cloud implementation? Rank up to your top five.”



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

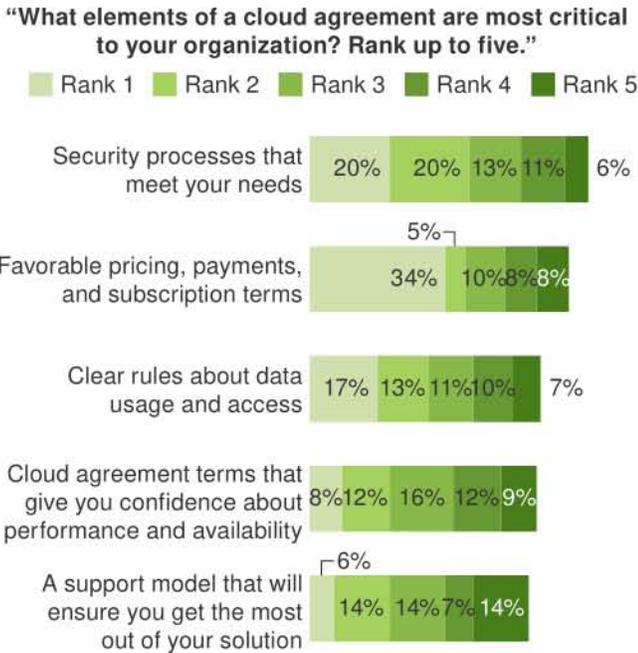
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

› **Almost half of respondents are adding more specific technical metrics; 41% are increasing standardization within a project.** To improve the quality of delivery and adherence to terms, cloud decision-makers are pushing for a number of changes in their cloud agreements. The top change is adding more technical metrics (47%), followed by requiring more regular status reports/meetings (43%) and adding more business outcome metrics (41%). Our study found that 41% of respondents are bucking the trend of customized agreements and instead beginning to use standard cloud agreements between providers on a project.

Forty-one percent of respondents are beginning to use standard cloud agreements between providers on a project.

› **Security and pricing are frequently the most important terms in a cloud agreement.** In the end, CSPs may not agree to all of their customers' preferred terms for deployments, and negotiations may turn into a “take it or leave it” conversation for some stipulations. While it's ideal to incorporate a standard list of terms to ensure optimal service levels, it's quite possible that contract decision-makers will need to prioritize the elements of cloud agreements that they believe are most valuable. Our study found that respondents tend to rate security processes (which presumably include compliance and privacy considerations) as the most important, followed by favorable pricing, payments, and subscription terms. Additional considerations include clear rules about data usage and access, terms that provide confidence about performance and availability, and a support model that will maximize success (see Figure 7).

FIGURE 7
Security, Pricing, Data Use, Reliability, And Support Are Key Considerations



Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization
 Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

FIGURE 8
Key Elements Of The ISO/IEC 19086-1 Standard

Area	Key elements
Performance	<ul style="list-style-type: none"> • Accessibility • Availability • Capacity • Elasticity
Service	<ul style="list-style-type: none"> • Service monitoring • Response time • Service resilience / fault tolerance • Disaster recovery • Backup and restore data • Cloud service support
Data management	<ul style="list-style-type: none"> • Cloud service provider data • Cloud service customer data • Intellectual property rights • Account data • Derived data • Data portability • Data deletion • Data location • Data examination
Governance	<ul style="list-style-type: none"> • Roles and responsibilities • Personally identifiable information • Information security • Termination of service • Changes to features and functionality • Law enforcement access • Attestation, certification, and audits

Source: ISO/IEC 19086-1 International Standard

Key Recommendations

With the ISO/IEC 19086-1 Standard being released in the fall of 2016, the ISO is addressing a substantial market requirement. In considering its usefulness, customers seeking to establish cloud agreements should embrace the following suggestions:

- › **Consult best practices guidance when negotiating cloud agreements.** Cloud service customers should start ensuring they have information they need from CSPs immediately. Published guidance such as Forrester's Cloud Contract Negotiations checklist suggests a range of considerations, from pricing and subscription terms to data usage, business continuity, security, support, SLAs, benchmarking, indemnification and liability, and upgrades.⁷ Use the ISO/IEC 19086-1 Standard for more guidance upon publication.
- › **Use ISO's best practices guidelines to guide agreement negotiations and cloud discussions.** When available, use the ISO/IEC 19086-1 Standard in a request for information and other communications with CSPs to support consistent transparency. Despite the ample contributions of industry analysts and other sources, the industry has suffered for the lack of a ready template for key issues for cloud agreements, and the proposed ISO standard fills a substantial market requirement. Use it as a guide for crafting your own agreements.
- › **Understand that the ISO standard covers a lot but not everything. Be ready to go beyond.** While appreciating the contribution of the proposed ISO standard, pay attention to other areas not addressed specifically by the standard. For example, customers continue to struggle with other areas of "legalese," including indemnification and limitations of liability. Consider the ISO standard as a guidance document; the considerations will need to be tailored to meet each agreement individually.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 467 organizations from Australia, Brazil, France, Germany, Japan, Korea, the UK, and the US to evaluate their service agreements with cloud service providers. Survey participants included cloud agreement decision-makers in IT, legal, operations, procurement, and risk management roles at enterprises, SMBs, and government organizations. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was conducted in June 2016.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"Organize The Chaos Of Cloud With A Realistic And Effective Strategy," Forrester Research, Inc., April 24, 2015

"The State Of Cloud Platform Standards: Q2 2015," Forrester Research, Inc., May 14, 2015

"Brief: Be Aware Of These Key Sourcing Trends," Forrester Research, Inc., February 27, 2015

"Brief: Cloud Contract Negotiations Checklist," Forrester Research, Inc., September 18, 2015

"Navigate The Limitations Of Public Cloud Agreements And SLAs," Forrester Research, Inc., July 25, 2013

Appendix C: Endnotes

¹ Source: "Benchmark Your Enterprise Cloud Adoption," Forrester Research, Inc., August 12, 2015.

² As of this writing the standard is in draft form, and is currently named the "Draft ISO/IEC JTC 19086-1 International Standard".

³ Source: "Brief: Be Aware Of These Key Sourcing Trends," Forrester Research, Inc., February 27, 2015.

⁴ Source: "TechRadar™: Data Security, Q1 2016," Forrester Research, Inc., March 17, 2016.

⁵ Source: "Brief: Be Aware Of These Key Sourcing Trends," Forrester Research, Inc., February 27, 2015.

⁶ Source: "Brief: Cloud Contract Negotiations Checklist," Forrester Research, Inc., September 18, 2015.

⁷ Source: "Brief: Cloud Contract Negotiations Checklist," Forrester Research, Inc., September 18, 2015.

Cloud Services Due Diligence Checklist

The multitude of cloud service options and service providers can cause challenges for organizations that want to move to the cloud and consume cloud services. The pressure caused by regulations and standards covering a wide range of topics—security, privacy, trust, personal information, and business-specific needs—further complicates these challenges.

Why use this Checklist?

This Checklist is based on international standard [ISO/IEC 19086-1](#), the Cloud Computing Service Level Agreement Framework. This Checklist can guide and help drive discussions about moving to the cloud. It will support your move to the cloud holistically and empower you to conduct a meaningful due diligence evaluation of cloud services.

Audience

- Risk Management
- Procurement
- Legal
- CIO



How to use the Checklist?

This Checklist raises key considerations as you move to the cloud. Different organizations and cloud projects should place different requirements for each element. In order to deploy the Checklist for cloud due diligence evaluations, organizations need to define the organizational cloud requirements for applicable Checklist elements, define the project specific requirements, and assess project options accordingly. Detailed guidance is available from the [instructional guide](#) for this Checklist.

Performance

Accessibility List accessibility standards, policies, and regulations met by the service.

Availability The percentage of time that the service is available and usable.

Capacity The number of simultaneous connections.
 The maximum capacity of resources.
 The number of inputs that will be processed over a period of time.
 The amount of data that will be transferred over a period of time.

Elasticity How fast and how precise the service can adjust to the amount of resources that are allocated.

Service

Service monitoring

- The parameters and mechanisms to monitor the service.

Response time

- The maximum, average, and variance in response time.

Service resilience/ fault tolerance

- The methods used to facilitate resilience and fault tolerance (include mean times, maximum times, and units of measurement).

Disaster recovery

- The maximum time required to restart the service in outage.
- The maximum time prior to a failure during which changes may be lost.
- The recovery procedures to restore the service and data.

Backup and restore data

- The number of data backups made in a period of time.
- The methods of backup and backup verification.
- The backup retention period.
- The number of backups retained.
- The location of backup storage.
- The number of restoration tests and the availability of test reports.
- The alternative methods for restoring data.

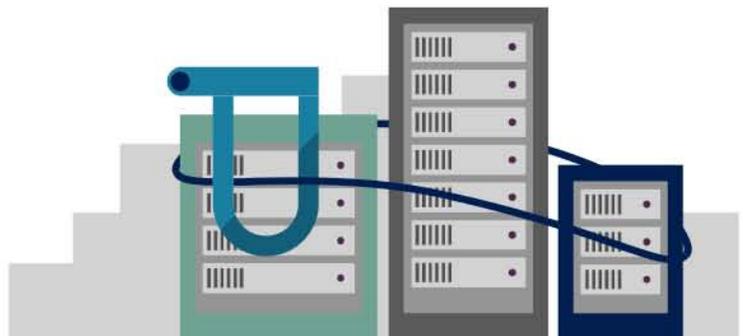
Cloud service support

- The available support plans, associated costs, and associated hours of operation.
- The specific contacts for service support.
- The service support methods (phone, web, tickets).
- For incident support: the incident support hours, levels of support, response time (average and maximum), reporting methods, and notification terms.



Data Management

- Cloud service provider data Define cloud service provider data.
-
- Cloud service customer data Define cloud service customer data and usage terms.
-
- Intellectual property rights Describe any intellectual property rights the cloud service provider claims on cloud customer data and vice versa.
-
- Account data List the required account data fields (names, addresses, etc.).
-
- Derived data Define the types of derived data and policies for use/access.
-
- Data portability Data portability capabilities including methods, formats and protocols.
-
- Data deletion Define the minimum and maximum times to completely delete cloud service customer data.
 Describe the data deletion process.
 Describe the data deletion notification policy.
-
- Data location List the geographic locations that data may be processed and stored, and if the cloud service customer can specify location requests.
-
- Data examination Describe how the cloud service provider examines cloud service customer data.



Governance

Roles and responsibilities

- The roles and responsibilities for the parties.

Personally identifiable information (PII)

- The PII protection standards met by the cloud service provider.

Information security

- The information security standards met by the cloud service provider.

Termination of service

- The process of notification of service termination, including the length of time that data and logs are retained after termination, the process for notification, and the return of assets.

Changes to features and functionality

- The minimum time between service change notification and implementation, and service change notification method.
- The minimum time period between the availability of a feature/function and the deprecation of that feature/function.

Law enforcement access

- The policy for responding to law enforcement requests of cloud service customer data.

Attestation, certification, and audits

- List/define the standards, policies, regulations, and applicable certifications that the cloud service provider attests to. Include audit schedule and location policies.

ISO/IEC 19086-1 Clause Mapping

Accessibility	Clause 10.2	Roles and responsibilities	Clause 9.5
Availability	Clause 10.3	PII	Clause 10.5
Capacity, Elasticity, Response time	Clause 10.4	Information security	Clause 10.6
Service monitoring	Clause 9.4	Termination of service	Clause 10.7
Service resilience/fault tolerance, Disaster recovery, Backup and restore data	Clause 10.11	Changes to features and functionality	Clause 10.10
Cloud service support	Clause 10.8	Law enforcement access	Clause 10.12
Data Privacy and sub-sections	Clause 10.12	Attestations, certifications, and audits	Clause 10.13

Please note that this Checklist is not intended to be and should not be considered a substitute for ISO/IEC 19086-1. To obtain access to the full text of this standard, please see the [ISO/IEC 19086-1](https://www.iso.org/standard/72431.html) webpage.

Study: Cloud Service Agreements Omit Key Considerations

New ISO/IEC 19086-1 Standard guides organizations to structured, effective agreements

CRITICAL CONSIDERATIONS FOR SELECTING CLOUD SERVICE PROVIDERS



Expertise in process and technology



Ability to integrate with apps



Industry-specific experience

KEY ELEMENTS OF THE ISO/IEC 19086-1 STANDARD AREN'T ALWAYS INCLUDED IN CLOUD AGREEMENTS

% of cloud contracts including each consideration



CLOUD BUYERS CARE ABOUT MORE THAN PRICE

Organizations rank the elements of cloud agreements that are most important to their organizations

70% Security processes that meet the organization's needs

65% Favorable pricing, payments, and subscription terms

58% Clear rules about data usage and access

57% Sufficient terms regarding performance and availability

ORGANIZATIONS ARE PRIMED TO ADOPT THE ISO/IEC 19086-1 STANDARD

Organizations prefer to follow best practices to ensure comprehensive agreements



Consult external guidance



Are increasing standardization of cloud agreements



Read the full study

Methodology: In this study, Forrester conducted an online survey of 467 organizations from Australia, Brazil, France, Germany, Japan, Korea, UK and US to evaluate their service agreements with cloud service providers. Survey participants included cloud agreement decision-makers in IT, legal, operations, procurement, and risk management roles at Enterprises, SMBs, and government organizations. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was conducted in June 2016.

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2016

Base: 467 respondents responsible for or involved in the decision-making process for cloud agreements within their organization

epic.org

EPIC-17-06-13-ICE-FOIA-20181003-2ndInterim-Production-pt1

000243

2018-ICLI-00030_243

PRIVACY POLICY FOR DHS MOBILE APPLICATIONS

I. Purpose

This Instruction implements the Department of Homeland Security (DHS or the Department) Directive 047-01, "Privacy Policy and Compliance," concerning DHS Mobile Applications intended for use by DHS employees and/or the public.

II. Scope

This Instruction applies throughout DHS for Mobile Applications that are developed by, on behalf of, or in coordination with the Department.

III. References

- A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note]
- B. Title 5, United States Code (U.S.C.), Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]
- C. Title 6, U.S.C., Section 142, "Privacy officer"
- D. Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014 (FISMA)]
- E. Title 15 U.S.C., Chapter 91, "Children's Online Privacy Protection Act"
- F. Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information"
- G. DHS Directive 047-01, "Privacy Policy and Compliance" (July 25, 2011)
- H. DHS Sensitive Systems Policy Directive 4300A (March 14, 2011)
- I. DHS Privacy policy guidance and requirements issued (as updated) by the Chief Privacy Officer and published on the Privacy Office website, including:

1. Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (December 29, 2008)
2. Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments (December 30, 2008)
3. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS (March 2012)

IV. Definitions

A. **DHS Carwash** is the service sponsored by DHS Office of the Chief Information Officer (OCIO) that provides development teams with a continuous integration, build, test, source code management, and issue tracking environment for building DHS Mobile Apps. The shared platform provides application lifecycle management and support for mobile apps built on development frameworks. The DHS Carwash also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility.

B. **DHS Mobile Application (DHS Mobile App)** means a native software application that is developed by, on behalf of, or in coordination with DHS for use on a mobile device (e.g., phone or tablet) by DHS employees and/or the public.

C. **Fair Information Practice Principles** means the policy framework adopted by the Department in Directive 047-01, Privacy Policy and Compliance, regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information, and as described in Privacy Policy Guidance Memorandum 2008-01.

D. **Location Information** means the ability of a mobile device to know a user's current location and/or location history as determined by Global Positioning System (GPS) and/or other methods.

E. **Metadata** means the information stored as the description of a unique piece of data and all the properties associated with it. For example, mobile device metadata may include the time and duration of all phone calls made from a particular mobile device, the mobile device IDs of the mobile devices involved in the phone calls, and the locations of each participant when the phone calls occurred.

F. **Mobile Device ID** means a unique serial number that is specific to a mobile device. These numbers vary in permanence, but typically a device has at least one permanent number. These numbers are used for various purposes, such as for security and fraud detection and remembering user preferences. Combining a unique device identifier with other information, such as location data, can allow the phone to be used as a tracking device.

G. **Personally Identifiable Information (PII)** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information may include a name, Social Security number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, biometric identifier (e.g., facial recognition, photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

H. **Privacy Compliance Documentation** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

I. **Privacy Compliance Review (PCR)** means both the DHS Privacy Office process to be followed and the document designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing Privacy Compliance Documentation including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

J. **Privacy Impact Assessment (PIA)** means both the DHS Privacy Office process to be followed and the document required whenever an information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information are used, stored, and shared, how the information may be accessed, how the information is protected from unauthorized use or disclosure, and how long it is retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may, in coordination with the affected component and the Office of the General Counsel,

modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

K. **Privacy Threshold Analysis (PTA)** means both the DHS Privacy Office process to be followed and the document used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the proposed use, identifies the legal authorities for the proposed use, and describes what PII, if any, is collected (and from whom) and how that information is used. PTAs are adjudicated by the Chief Privacy Officer.

L. **Program Manager** means the responsible agency representative, who, with significant discretionary authority, is uniquely empowered to make final scope-of-work, capital investment, and performance acceptability decisions.

M. **Sensitive Content** means information that may not be PII, but raises privacy concerns because it may be related to the use of PII (e.g., location information, mobile device ID, or metadata).

N. **Sensitive Personally Identifiable Information (SPII)** means PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as Social Security Number (SSNs), Alien Registration Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are SPII if DHS maintains them in conjunction with other identifying information about the individual. In some instances the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be SPII, but could be if it is a list of employees who received poor performance ratings.

O. **System Manager** means the individual identified in a System of Records Notice who is responsible for the operation and management of the system of records to which the System of Records Notice pertains.

P. **System of Records Notice (SORN)** means the statement providing the public notice of the existence and character of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system are included.

Q. **User** means a person using a DHS Mobile App.

V. Responsibilities

- A. The **Chief Privacy Officer** is responsible for:
1. Working with Component Privacy Officers and Privacy Points of Contact (PPOCs) to provide guidance and ensure that DHS Mobile Apps are in compliance with DHS privacy policies;
 2. Reviewing and approving Privacy Compliance Documentation for DHS Mobile Apps, as appropriate; and
 3. Performing periodic PCRs of DHS Mobile Apps to ascertain compliance with DHS privacy policy.
- B. The **Chief Information Officer** is responsible for:
1. Providing web technology services, security, and technical assistance for the development of DHS Mobile Apps;
 2. Ensuring that DHS Mobile Apps comply with FISMA and DHS Sensitive Systems Policy Directive 4300A; and
 3. Performing iterative scans and tests on the source code of DHS Mobile Apps through the DHS Carwash process in order to provide insight on code security, quality, and accessibility.
- C. **Component Privacy Officers** are responsible for:
1. Coordinating with Program Managers or System Managers, as appropriate, together with the Chief Privacy Officer and counsel to complete Privacy Compliance Documentation, as necessary, for all proposed DHS Mobile Apps; and
 2. Collaborating with the Chief Privacy Officer in conducting Privacy Compliance Reviews.
- D. **Privacy Points of Contact (PPOCs)** are responsible for assuming the duties of Component Privacy Officers in Components that do not have Privacy Officers.

E. **Program Managers, or System Managers**, as appropriate, are responsible for:

1. Coordinating with the Component Privacy Officer or PPOC to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any DHS Mobile Apps;
2. Engaging and coordinating with the OCIO Carwash team to ensure that DHS Mobile Apps are sent through DHS Carwash process when proposing, developing, implementing or changing any DHS Mobile Apps;
3. Coordinating with the Component Privacy Officer or PPOC and counsel to prepare drafts of all Privacy Compliance Documentation, as necessary, when proposing, developing, implementing, or changing any DHS Mobile Apps;
4. Monitoring the design, deployment, operation, and retirement of DHS Mobile Apps to ensure that the collection and use of PII and Sensitive Content, if any, is limited to what is described in the Privacy Compliance Documentation; and
5. Coordinating with the Component Privacy Officer or PPOC and the DHS Office for Civil Rights and Civil Liberties to establish administrative, technical, and physical controls for storing and safeguarding PII and Sensitive Content consistent with DHS privacy, security, and records management requirements to ensure the protection of PII and Sensitive Content from unauthorized access, disclosure, or destruction as it relates to DHS Mobile Apps.

VI. Content and Procedures

A. **Minimum Privacy Requirements for DHS Mobile Apps**: The policies detailed below provide the baseline privacy requirements for DHS Mobile Apps. Additional privacy protections may be necessary depending on the purpose and capabilities of each individual mobile app.

1. Provide Notice
 - a. **App-Specific Privacy Policy (see Appendix A)**: DHS Mobile Apps have a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the DHS website Privacy Policy.

The Privacy Policy should briefly describe the app's information practices to include the collection, use, sharing, disclosure, and retention of PII, SPII, and Sensitive Content. The Privacy Policy should also address: redress procedures, app security, and the Children's Online Privacy Protection Act (if applicable).

b. Privacy Statement: If a DHS Mobile App is collecting PII from users, then a Privacy Statement is provided at the point of collection. This Privacy Statement may be provided through a pop-up notification on the DHS Mobile App screens where PII is collected or via another mechanism approved by the Chief Privacy Officer.

c. Contextual Notice: DHS Mobile Apps deliver direct, contextual, self-contained notice about the uses of information through the mobile platform. Therefore, these notices should be:

(1) Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app;

(2) Provided as "just-in-time" disclosures and obtain users' affirmative express consent before a DHS Mobile App accesses Sensitive Content or other tools and applications on the mobile device for the first time (e.g., location services); and

(3) Provided with independent opt-out features so that users may customize the mobile app's features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate.

2. Limit the Collection and/or Use of Sensitive Content

a. DHS Mobile App features cannot collect and/or use PII, SPII, or Sensitive Content, unless directly needed to achieve a DHS mission purpose; and

b. If the collection and/or use of PII, SPII, or Sensitive Content is directly necessary to achieve a DHS mission purpose, then the collection and/or use of the information is documented and justified in the mobile app's Privacy Compliance Documentation.

3. Establish Guidelines for User Submitted Information
 - a. Where feasible, use forms and check boxes to limit data collection and minimize data entry errors;
 - b. Before allowing a user to submit information to DHS, provide a “review before sending” function that allows users to correct or opt-out of sending their information to the Department; and
 - c. Unless necessary to achieve a DHS mission purpose, limit the ability of users to post information within the app that other users may access or view. This limits the potential for users to share PII, SPII, or Sensitive Content unnecessarily.
4. Ensure Mobile App Security and Privacy
 - a. Engage with the DHS Carwash throughout development to ensure the security and privacy of the mobile app;
 - b. If users submit information through a DHS Mobile App, that information is encrypted in transit and immediately transferred to a protected internal DHS system that is compliant with existing DHS IT security policy; and
 - c. Sensitive content that a DHS Mobile App accesses or uses for the benefit of the user, but that DHS does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device. This information should not be transmitted to or shared with DHS.

B. DHS Mobile App Development:

1. Program Managers and System Managers notify their Component Privacy Officers or PPOCs and the OCIO Carwash team before engaging in the development of a DHS Mobile App.
2. Component Privacy Officers or PPOCs engage with Program Managers and System Managers to ensure privacy protections outlined in Section VI. A. of this document are integrated into the development of the DHS Mobile App.
3. Before deployment, the DHS Mobile App goes through the DHS Carwash.
4. The OCIO Carwash team provides the iterative scan results of the DHS Carwash to the Program Managers and System Managers.

5. Before deployment, Program Managers and System Managers in consultation with Component Privacy Officers or PPOCs complete a PTA, an App-Specific Privacy Policy, and a Privacy Statement (if necessary) for the DHS Mobile App. The PTA (a) documents a general description of the proposed use, (b) identifies the legal authorities for the proposed use and (c) describes what PII, if any, is collected, from whom PII is collected and how the PII is used. Component Privacy Officers or PPOCs compare this PTA to the DHS Carwash iterative scan results to ensure the PTA accurately describes the DHS Mobile App's collection, use, maintenance, retention, disclosure, deletion and destruction of PII, SPII, and Sensitive Content.

6. Before deployment, the DHS Mobile App's PTA, App-Specific Privacy Policy, Privacy Statement (if necessary), and results of the DHS Carwash iterative scans are submitted to the Chief Privacy Officer for a prompt review and evaluation to determine whether the DHS Mobile App contains appropriate privacy protections and whether a new or updated PIA, SORN, or other Privacy Compliance Documentation is required.

7. Once it is determined that all necessary Privacy Compliance Documentation is complete and that the DHS Mobile App contains appropriate privacy protections, the Chief Privacy Officer provides approval for the release of the DHS Mobile App.

8. DHS Mobile Apps go through the DHS Carwash any time there is a change made to the DHS Mobile App that affects or potentially affects the collection and use of PII, SPII, or Sensitive Content and consistent with the PTA review cycle. Existing DHS Mobile Apps, which were developed before the implementation of this policy, go through the DHS Carwash within 6 months of this policy's issue date. Program Managers and System Managers provide the DHS Carwash results, pertaining to their particular DHS Mobile App, to the Chief Privacy Officer for a prompt review and evaluation to ensure that the DHS Mobile App continues to contain appropriate privacy protections.

C. **Retention of PII:** Component Program Managers or System Managers, where appropriate, maintain PII collected through DHS Mobile Apps in accordance with approved records retention schedules.

D. **Privacy Compliance Reviews (PCR):** The Chief Privacy Officer, in collaboration with Component Privacy Officers or PPOCs, may conduct PCRs of DHS Mobile Apps periodically, at the sole discretion of the Chief Privacy Officer, to ascertain compliance with DHS privacy policy.

VII. Questions

Address any questions or concerns regarding these Instructions to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.



Karen L. Neuman
Chief Privacy Officer

March 30, 2016
Date

Privacy Policy
For the
[INSERT NAME] Mobile Application

Overview

The overview should be a single paragraph that is used to describe the DHS Mobile Application ("DHS Mobile App"). It should include the name of the DHS component that developed the app as well as the name of the DHS Mobile App, itself. This overview should also provide a brief description of the DHS Mobile App's purpose and function.

Information Collected

Provide the categories of individuals for whom information is collected, and for each category, list all information, including PII, SPII, and Sensitive Content that is collected by the DHS Mobile App. Details regarding the retention of information collected by the DHS Mobile App should also be addressed in this section.

Uses of Information

List each use (internal and external to the Department) of the information collected or maintained by the DHS Mobile App. Provide a detailed response that states how and why the different data elements is used.

Information Sharing

Discuss the external Departmental sharing of information (e.g., DHS to FBI). External sharing encompasses sharing with other federal, state and local government, and private sector entities.

Application Security

Discuss the technical safeguards and security controls, specific to the particular DHS Mobile App, in place to protect information that is collected and/or maintained by the DHS Mobile App.

How to Access or Correct your Information

Provide information about the processes in place for users of the DHS Mobile App to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

Analytics Tools

Discuss any analytics tools that the DHS Mobile App may use. This should include a description of any information collected through these analytic capabilities.

Privacy Policy Contact Information

Provide component privacy office contact information so that users may provide feedback and/or ask questions in regards to this DHS Mobile App Privacy Policy. This contact information may include the component privacy office's phone number, email, and mailing address.

ICE Privacy Division
Information Governance and Privacy (IGP)
Mobile Applications
February 2017

DHS Privacy Policy for DHS Mobile Applications (March 30, 2016) sets forth the requirements for developing and operating a Mobile Application (Mobile App). There is no corresponding ICE policy. All Mobile Apps¹ need to comply with the policy.

Privacy Division Review Checklist:

- App-Specific Privacy Threshold Analysis (PTA)** – In addition to a description, the PTA should include a brief explanation of any discrepancies noted in the Carwash reports and the platforms on which the Mobile App can be downloaded (e.g., Google Play, Apple Store, etc.).
- Carwash Reports** – The executable file² for the Mobile App should be submitted to the ICE Carwash Coordinator at (b)(7)(E). The System Owners can work directly with the ICE Carwash Coordinator to submit the file. Review the reports alongside the PTA and check for any discrepancies.
- App-Specific Privacy Policy** – Mobile Apps need a Privacy Policy that is easily accessible to users through the commercial app store before the installation as well as within the app, itself, after installation. The Privacy Policy should be app-specific and cannot merely reference the ICE website Privacy Policy. A Privacy Policy template is attached.
- Contextual Notice** – Mobile Apps should deliver direct, contextual, self-contained notice about the uses of information through the mobile platform. Notices should be:
 - Provided upon each update to specifically identify any changes to the use of information from previous versions of the Mobile App;
 - Provided as “just-in-time” disclosures and obtain users’ affirmative express consent before the Mobile App accesses Sensitive Content or other tools and applications on the mobile device for the first time (e.g., location services); and
 - Provides as independent opt-out features so that users may customize the mobile app’s features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate.

If applicable:

- Privacy Statement** – If the Mobile App is collecting personally identifiable information (PII) from users, then a Privacy Statement is required at the point of collection. The Privacy Statement may be provided through a pop-up notification on the Mobile App screen where PII is collected or via another mechanism with prior approval.
- Guidelines for User Submitted Information**
 - Where feasible, the Mobile App should use forms and check boxes to limit data collection and minimize data entry errors;
 - Before allowing a user to submit information to ICE, the Mobile App should provide a “review before sending” function that allows users to correct or opt-out of sending their information; and
 - Unless necessary to achieve an ICE mission purpose, limit the ability of users to post information within the Mobile App that other users may access or view.

¹ Mobile Apps are native software applications that are developed by, on behalf of, or in coordination with DHS for use on a mobile device by DHS employees and/or the public. Native applications are installed through an application store (such as Google Play or Apple’s App Store). They are developed specifically for a platform and can take full advantage of all the device features (e.g., they can use the camera, GPS, compass, list of contacts, etc.)

² The Mobile App may be available on multiple platforms thus there may be more than one executable file. Work with the ICE Carwash Coordinator to ensure all versions of go through the Carwash.

PRIVACY POLICY TEMPLATE

Privacy Policy [INSERT NAME] Mobile Application

Overview

The overview should be a single paragraph that is used to describe the Mobile Application ("Mobile App"). It should include the name of the component that developed the app as well as the name of the Mobile App, itself. This overview should also provide a brief description of the Mobile App's purpose and function.

Information Collected

Provide the categories of individuals for whom information is collected, and for each category, list all information, including PII, SPII, and Sensitive Content that is collected by the Mobile App. Details regarding the retention of information collected by the Mobile App should also be addressed in this section.

Uses of Information

List each use (internal and external to the Department) of the information collected or maintained by the Mobile App. Provide a detailed response that states how and why the different data elements are used.

Information Sharing

Discuss the external Departmental sharing of information (e.g., HSI to FBI). External sharing encompasses sharing with other federal, state and local government, and private sector entities.

Application Security

Discuss the technical safeguards and security controls, specific to the particular Mobile App, in place to protect information that is collected and/or maintained by the Mobile App.

Analytics Tools

Discuss any analytics tools that the Mobile App may use. This should include a description of any information collected through these analytic capabilities.

How to Access or Correct your Information

Individuals may access information collected and maintained by ICE through the Privacy Act and the Freedom of Information Act (FOIA) processes. Individuals seeking notification of, access to, or correction of any record collected by the Mobile App may submit a request in writing to the ICE FOIA Officer, by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, DC 20536-5009
(866) 633-1182
<https://www.ice.gov/foia>

Privacy Policy Contact Information

If you have any questions or suggestions regarding our privacy policy, please contact the ICE Office of Information Governance and Privacy at (b)(7)(E) or mail them to Office of Information Governance and Privacy, U.S. Immigration and Customs Enforcement, 500 12th Street SW, Mail Stop 5004, Washington, DC 20536-5004.

Last Update

This Privacy Policy was most recently updated on [DATE], effective [DATE]. It was edited on [DATE] to reflect [CHANGES].



**Privacy Impact Assessment Update for
CBP Border Searches of Electronic
Devices**

DHS/CBP/PIA-008(a)

January 4, 2018

Contact Point

John Wagner

Deputy Executive Assistant Commissioner

Office of Field Operations

U.S. Customs and Border Protection

(202) 344-1610

Reviewing Official

Philip S. Kaplan

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

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

Overview

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

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

¹ Pursuant to CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018), an electronic device is any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players.

² CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (January 2018). The 2009 Directive included a requirement to review the policy, as did the original Privacy Impact Assessment (*See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), available at www.dhs.gov/privacy).

³ CBP's statutorily-prescribed duties include, among other things, ensuring the interdiction of persons and goods illegally entering or exiting the United States; enforcing the customs and trade laws of the United States; detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States; and safeguarding the border of the United States to protect against the entry of dangerous goods. 6 U.S.C. § 211.

⁴ *See* DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), available at www.dhs.gov/privacy.



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

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

Border Search Authority

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

⁵ See DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), *available at* www.dhs.gov/privacy.

⁶ See *Cotterman v. United States*, 709 F.3d 952 (9th Cir. 2013).



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

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

If Selected for a Search of Your Electronic Device

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

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

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

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

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



that all vehicles, other conveyances, persons, baggage, packages, or other containers are subject to detention and search. Specifically regarding border searches of electronic devices, CBP has created a tear-sheet¹⁰ to provide travelers who have questions or concerns regarding the search of their electronic device.

Reason for the PIA Update

CBP previously published a PIA¹¹ examining the privacy impact of the procedures for searching electronic devices at the border in 2009. In the ensuing years, there have been a number of significant developments, including:

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

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

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

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

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

¹¹ See DHS/CBP/PIA-008 Border Searches of Electronic Devices (August 25, 2009), available at www.dhs.gov/privacy.



A. Types of CBP Border Searches of Electronic Devices

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

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

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

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

Basic Search

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



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

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

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

Advanced Search

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

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

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

¹² CBP Directive No. 3340-049A at 5.1.3.

¹³ CBP Directive No. 3340-049A at 5.1.4.



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

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

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

i. Reasonable Suspicion or National Security Concern

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

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

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

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

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



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

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

iii. Treatment of Privileged Information

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

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

¹⁶ CBP Directive No. 3340-049A at 5.1.2.

¹⁷ CBP Directive No. 3340-049A at 5.1.2.

¹⁸ CBP Directive No. 3340-049A at 5.1.2.



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

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

iv. Handling of Passcode-Protected or Encrypted Information

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

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

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

¹⁹ CBP Directive No. 3340-049A at 5.2.1.1.

²⁰ CBP Directive No. 3340-049A at 5.2.1.2.

²¹ CBP Directive No. 3340-049A at 5.2.1.3.

²² CBP Directive No. 3340-049A at 5.3.1.

²³ CBP Directive No. 3340-049A at 5.3.2.



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

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

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

The 2009 Directive provided for the retention of information relating to immigration, customs, and other enforcement matters, if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. Since that time, CBP published a Privacy Impact Assessment Update regarding CBP's use of the Automated Targeting System (ATS)²⁴ to store information copied and stored from a traveler's electronic device. To further CBP's border security mission, CBP may use ATS to further review, analyze, and assess the information physically resident on the electronic devices, or copies thereof, that CBP collected from individuals who are of significant law enforcement, counterterrorism, or other national security concerns. CBP may retain information from the physical device and the report containing the analytical results, which are relevant to immigration, customs, and/or other enforcement matters, in the ATS-Targeting Framework (TF) for purposes of CBP's border security mission, including identifying individuals who and cargo that need additional scrutiny. CBP may use ATS-TF to vet the information collected from the electronic devices of individuals of concern against CBP holdings and create a report which includes data that may be linked to illicit activity or actors. Information from electronic devices uploaded into ATS will be normalized²⁵ and flagged as originating from an electronic device.

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

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

²⁴ See DHS/CBP/PIA-006 Automated Targeting System (ATS), available at www.dhs.gov/privacy.

²⁵ Normalization is the process of organizing data in a database to reduce redundancy and ensure that related items are stored together.



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

Fair Information Practice Principles (FIPPs)

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

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

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

1. Principle of Transparency

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

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

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



detention and search. CBP has created a tear-sheet²⁷ to provide travelers who have questions or concerns regarding the search of their electronic device. CBP has also published its previous, and newly updated, policies regarding border searches of electronic devices, and is publishing this PIA in tandem. CBP has also posted information on its website regarding the issue of border searches of electronic devices.²⁸

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

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

- DHS/CBP-006 Automated Targeting System³⁰ 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 TECS³¹ covers among other things, any records of any inspections conducted at the border by CBP, including inspections of electronic devices, including factors on the initiation of the search as described in the TECS Electronic Media Report module.
- DHS/CBP-013 Seized Assets and Case Tracking System (SEACATS)³² provides notice regarding any seizures, fines, penalties, or forfeitures associated with the seizure of electronic devices.

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

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

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

²⁹ CBP Directive at 5.4.1.3.

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

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

³² DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.



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

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

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

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

2. Principle of Individual Participation

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

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

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

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

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



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

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

3. Principle of Purpose Specification

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

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

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

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

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

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

³⁸ *See, e.g., United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *United States v. 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.³⁹ Persons and merchandise encountered by CBP at the international border are not only subject to inspection under U.S. law, they also have been or will be abroad and generally subject to the legal authorities of at least one other sovereign.⁴⁰

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

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

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

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

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

⁴⁰ See *Boumelhem*, 339 F.3d at 423.

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

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



4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

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

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

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

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



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

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

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

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

5. Principle of Use Limitation

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

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



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

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

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

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

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

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

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



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

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

6. Principle of Data Quality and Integrity

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

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

⁴³ CBP Directive No. 3340-049A at 5.3.1.

⁴⁴ CBP Directive No. 3340-049A at 5.3.2.

⁴⁵ DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764.



7. Principle of Security

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

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

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

8. Principle of Accountability and Auditing

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

As a matter of policy, CBP has created robust auditing and accountability measures for this program, in part due to the heightened privacy concerns regarding border searches of electronic devices. All Officers performing a border search are responsible for completing all after-action reporting requirements. This responsibility includes ensuring the completion of all applicable documentation such as the Customs Form (CF) 6051D⁴⁷ when appropriate, and creation and/or

⁴⁶ CBP Directive No. 3340 at 5.5.1.5.

⁴⁷ Customs Form (CF) 6051D is provided to the traveler as a receipt. This form contains contact information for the traveler and the CBP Officer to ensure each party can contact the other with questions or for retrieval of the electronic device at the conclusion of the border search. From the time the electronic device is detained to the time it is returned to the traveler, the device is kept in secured facilities with restricted access at all times.



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

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

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

The updated policy directive also directs that the CBP Management Inspection⁴⁹ will develop and periodically administer an auditing mechanism to review whether border searches of electronic devices are being conducted in conformity with this Directive. In addition, the CBP Privacy Officer shall conduct a CBP Privacy Evaluation of the privacy controls noted above in the PIA.

Responsible Official

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

Approval Signature

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

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

⁴⁸ 6 U.S.C. § 211(k)(5).

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

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

Department of Homeland Security
DHS Directives System
Instruction Number: 047-01-003
Revision Number: 00
Issue Date: March 30, 2016

I. Purpose

This Instruction implements the Department of Homeland Security (DHS or the Department) Directive 047-01, "Privacy Policy and Compliance," concerning DHS Mobile Applications intended for use by DHS employees and/or the public.

II. Scope

This Instruction applies throughout DHS for Mobile Applications that are developed by, on behalf of, or in coordination with the Department.

III. References

- A. Public Law 107-347, "E-Government Act of 2002," as amended, Section 208 [44 U.S.C. § 3501 note]
- B. Title 5, United States Code (U.S.C.), Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]
- C. Title 6, U.S.C., Section 142, "Privacy officer"
- D. Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014 (FISMA)]
- E. Title 15 U.S.C., Chapter 91, "Children's Online Privacy Protection Act"
- F. Title 6, C.F.R., Chapter 1, Part 5, "Disclosure of records and information"
- G. DHS Directive 047-01, "Privacy Policy and Compliance" (July 25, 2011)
- H. DHS Sensitive Systems Policy Directive 4300A (March 14, 2011)
- I. DHS Privacy policy guidance and requirements issued (as updated) by the Chief Privacy Officer and published on the Privacy Office website, including:
 - 1. Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the

Department of Homeland Security (December 29, 2008)

2. Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments (December 30, 2008)

3. Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS (March 2012)

IV. Definitions

A. **DHS Carwash** is the service sponsored by DHS Office of the Chief Information Officer (OCIO) that provides development teams with a continuous integration, build, test, source code management, and issue tracking environment for building DHS Mobile Apps. The shared platform provides application lifecycle management and support for mobile apps built on development frameworks. The DHS Carwash also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility.

B. **DHS Mobile Application (DHS Mobile App)** means a native software application that is developed by, on behalf of, or in coordination with DHS for use on a mobile device (e.g., phone or tablet) by DHS employees and/or the public.

C. **Fair Information Practice Principles** means the policy framework adopted by the Department in Directive 047-01, Privacy Policy and Compliance, regarding the collection, use, maintenance, disclosure, deletion, or destruction of Personally Identifiable Information, and as described in Privacy Policy Guidance Memorandum 2008-01.

D. **Location Information** means the ability of a mobile device to know a user's current location and/or location history as determined by Global Positioning System (GPS) and/or other methods.

E. **Metadata** means the information stored as the description of a unique piece of data and all the properties associated with it. For example, mobile device metadata may include the time and duration of all phone calls made from a particular mobile device, the mobile device IDs of the mobile devices involved in the phone calls, and the locations of each participant when the phone calls occurred.

F. **Mobile Device ID** means a unique serial number that is specific to a mobile device. These numbers vary in permanence, but typically a device has at least one permanent number. These numbers are used for various purposes, such as for security and fraud detection and remembering user preferences. Combining a unique device identifier with other information, such as location data, can allow the phone to be used as a tracking device.

G. **Personally Identifiable Information (PII)** means any information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual.

For example, when linked or linkable to an individual, such information may include a name, Social Security number, date and place of birth, mother's maiden name, Alien Registration Number, account number, license number, vehicle identifier number, license plate number, biometric identifier (e.g., facial recognition, photograph, fingerprint, iris scan, voice print), educational information, financial information, medical information, criminal or employment information, information created specifically to identify or authenticate an individual (e.g., a random generated number).

H. **Privacy Compliance Documentation** means any document required by statute or by the Chief Privacy Officer that supports compliance with DHS privacy policy, procedures, or requirements, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), Notices of Proposed Rulemaking for Exemption from certain aspects of the Privacy Act (NPRM), and Final Rules for Exemption from certain aspects of the Privacy Act.

I. **Privacy Compliance Review (PCR)** means both the DHS Privacy Office process to be followed and the document designed to provide a constructive mechanism to improve a DHS program's ability to comply with assurances made in existing Privacy Compliance Documentation including Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreement.

J. **Privacy Impact Assessment (PIA)** means both the DHS Privacy Office process to be followed and the document required whenever an information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of PII or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer. A PIA describes what information DHS is collecting, why the information is being collected, how the information are used, stored, and shared, how the information may be accessed, how the information is protected from unauthorized use or disclosure, and how long it is retained. A PIA also provides an analysis of the privacy considerations posed and the steps DHS has taken to mitigate any impact on privacy. As a general rule, PIAs are public documents. The Chief Privacy Officer may, in coordination with the affected component and the Office of the General Counsel,

modify or waive publication for security reasons, or to protect classified, sensitive, or private information included in a PIA.

K. **Privacy Threshold Analysis (PTA)** means both the DHS Privacy Office process to be followed and the document used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the proposed use, identifies the legal authorities for the proposed use, and describes what PII, if any, is collected (and from whom) and how that information is used. PTAs are adjudicated by the Chief Privacy Officer.

L. **Program Manager** means the responsible agency representative, who, with significant discretionary authority, is uniquely empowered to make final scope-of-work, capital investment, and performance acceptability decisions.

M. **Sensitive Content** means information that may not be PII, but raises privacy concerns because it may be related to the use of PII (e.g., location information, mobile device ID, or metadata).

N. **Sensitive Personally Identifiable Information (SPII)** means PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as Social Security Number (SSNs), Alien Registration Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are SPII if DHS maintains them in conjunction with other identifying information about the individual. In some instances the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be SPII, but could be if it is a list of employees who received poor performance ratings.

O. **System Manager** means the individual identified in a System of Records Notice who is responsible for the operation and management of the system of records to which the System of Records Notice pertains.

P. **System of Records Notice (SORN)** means the statement providing the public notice of the existence and character of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system are included.

Q. **User** means a person using a DHS Mobile App.

V. Responsibilities

- A. The **Chief Privacy Officer** is responsible for:
1. Working with Component Privacy Officers and Privacy Points of Contact (PPOCs) to provide guidance and ensure that DHS Mobile Apps are in compliance with DHS privacy policies;
 2. Reviewing and approving Privacy Compliance Documentation for DHS Mobile Apps, as appropriate; and
 3. Performing periodic PCRs of DHS Mobile Apps to ascertain compliance with DHS privacy policy.
- B. The **Chief Information Officer** is responsible for:
1. Providing web technology services, security, and technical assistance for the development of DHS Mobile Apps;
 2. Ensuring that DHS Mobile Apps comply with FISMA and DHS Sensitive Systems Policy Directive 4300A; and
 3. Performing iterative scans and tests on the source code of DHS Mobile Apps through the DHS Carwash process in order to provide insight on code security, quality, and accessibility.
- C. **Component Privacy Officers** are responsible for:
1. Coordinating with Program Managers or System Managers, as appropriate, together with the Chief Privacy Officer and counsel to complete Privacy Compliance Documentation, as necessary, for all proposed DHS Mobile Apps; and
 2. Collaborating with the Chief Privacy Officer in conducting Privacy Compliance Reviews.
- D. **Privacy Points of Contact (PPOCs)** are responsible for assuming the duties of Component Privacy Officers in Components that do not have Privacy Officers.

E. **Program Managers, or System Managers**, as appropriate, are responsible for:

1. Coordinating with the Component Privacy Officer or PPOC to ensure that privacy is appropriately addressed when proposing, developing, implementing, or changing any DHS Mobile Apps;
2. Engaging and coordinating with the OCIO Carwash team to ensure that DHS Mobile Apps are sent through DHS Carwash process when proposing, developing, implementing or changing any DHS Mobile Apps;
3. Coordinating with the Component Privacy Officer or PPOC and counsel to prepare drafts of all Privacy Compliance Documentation, as necessary, when proposing, developing, implementing, or changing any DHS Mobile Apps;
4. Monitoring the design, deployment, operation, and retirement of DHS Mobile Apps to ensure that the collection and use of PII and Sensitive Content, if any, is limited to what is described in the Privacy Compliance Documentation; and
5. Coordinating with the Component Privacy Officer or PPOC and the DHS Office for Civil Rights and Civil Liberties to establish administrative, technical, and physical controls for storing and safeguarding PII and Sensitive Content consistent with DHS privacy, security, and records management requirements to ensure the protection of PII and Sensitive Content from unauthorized access, disclosure, or destruction as it relates to DHS Mobile Apps.

VI. Content and Procedures

A. **Minimum Privacy Requirements for DHS Mobile Apps**: The policies detailed below provide the baseline privacy requirements for DHS Mobile Apps. Additional privacy protections may be necessary depending on the purpose and capabilities of each individual mobile app.

1. Provide Notice
 - a. **App-Specific Privacy Policy (see Appendix A)**: DHS Mobile Apps have a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the DHS website Privacy Policy.

The Privacy Policy should briefly describe the app's information practices to include the collection, use, sharing, disclosure, and retention of PII, SPII, and Sensitive Content. The Privacy Policy should also address: redress procedures, app security, and the Children's Online Privacy Protection Act (if applicable).

b. Privacy Statement: If a DHS Mobile App is collecting PII from users, then a Privacy Statement is provided at the point of collection. This Privacy Statement may be provided through a pop-up notification on the DHS Mobile App screens where PII is collected or via another mechanism approved by the Chief Privacy Officer.

c. Contextual Notice: DHS Mobile Apps deliver direct, contextual, self-contained notice about the uses of information through the mobile platform. Therefore, these notices should be:

(1) Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app;

(2) Provided as "just-in-time" disclosures and obtain users' affirmative express consent before a DHS Mobile App accesses Sensitive Content or other tools and applications on the mobile device for the first time (e.g., location services); and

(3) Provided with independent opt-out features so that users may customize the mobile app's features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate.

2. Limit the Collection and/or Use of Sensitive Content

a. DHS Mobile App features cannot collect and/or use PII, SPII, or Sensitive Content, unless directly needed to achieve a DHS mission purpose; and

b. If the collection and/or use of PII, SPII, or Sensitive Content is directly necessary to achieve a DHS mission purpose, then the collection and/or use of the information is documented and justified in the mobile app's Privacy Compliance Documentation.

3. Establish Guidelines for User Submitted Information
 - a. Where feasible, use forms and check boxes to limit data collection and minimize data entry errors;
 - b. Before allowing a user to submit information to DHS, provide a “review before sending” function that allows users to correct or opt-out of sending their information to the Department; and
 - c. Unless necessary to achieve a DHS mission purpose, limit the ability of users to post information within the app that other users may access or view. This limits the potential for users to share PII, SPII, or Sensitive Content unnecessarily.
4. Ensure Mobile App Security and Privacy
 - a. Engage with the DHS Carwash throughout development to ensure the security and privacy of the mobile app;
 - b. If users submit information through a DHS Mobile App, that information is encrypted in transit and immediately transferred to a protected internal DHS system that is compliant with existing DHS IT security policy; and
 - c. Sensitive content that a DHS Mobile App accesses or uses for the benefit of the user, but that DHS does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device. This information should not be transmitted to or shared with DHS.

B. DHS Mobile App Development:

1. Program Managers and System Managers notify their Component Privacy Officers or PPOCs and the OCIO Carwash team before engaging in the development of a DHS Mobile App.
2. Component Privacy Officers or PPOCs engage with Program Managers and System Managers to ensure privacy protections outlined in Section VI. A. of this document are integrated into the development of the DHS Mobile App.
3. Before deployment, the DHS Mobile App goes through the DHS Carwash.
4. The OCIO Carwash team provides the iterative scan results of the DHS Carwash to the Program Managers and System Managers.

5. Before deployment, Program Managers and System Managers in consultation with Component Privacy Officers or PPOCs complete a PTA, an App-Specific Privacy Policy, and a Privacy Statement (if necessary) for the DHS Mobile App. The PTA (a) documents a general description of the proposed use, (b) identifies the legal authorities for the proposed use and (c) describes what PII, if any, is collected, from whom PII is collected and how the PII is used. Component Privacy Officers or PPOCs compare this PTA to the DHS Carwash iterative scan results to ensure the PTA accurately describes the DHS Mobile App's collection, use, maintenance, retention, disclosure, deletion and destruction of PII, SPII, and Sensitive Content.

6. Before deployment, the DHS Mobile App's PTA, App-Specific Privacy Policy, Privacy Statement (if necessary), and results of the DHS Carwash iterative scans are submitted to the Chief Privacy Officer for a prompt review and evaluation to determine whether the DHS Mobile App contains appropriate privacy protections and whether a new or updated PIA, SORN, or other Privacy Compliance Documentation is required.

7. Once it is determined that all necessary Privacy Compliance Documentation is complete and that the DHS Mobile App contains appropriate privacy protections, the Chief Privacy Officer provides approval for the release of the DHS Mobile App.

8. DHS Mobile Apps go through the DHS Carwash any time there is a change made to the DHS Mobile App that affects or potentially affects the collection and use of PII, SPII, or Sensitive Content and consistent with the PTA review cycle. Existing DHS Mobile Apps, which were developed before the implementation of this policy, go through the DHS Carwash within 6 months of this policy's issue date. Program Managers and System Managers provide the DHS Carwash results, pertaining to their particular DHS Mobile App, to the Chief Privacy Officer for a prompt review and evaluation to ensure that the DHS Mobile App continues to contain appropriate privacy protections.

C. **Retention of PII:** Component Program Managers or System Managers, where appropriate, maintain PII collected through DHS Mobile Apps in accordance with approved records retention schedules.

D. **Privacy Compliance Reviews (PCR):** The Chief Privacy Officer, in collaboration with Component Privacy Officers or PPOCs, may conduct PCRs of DHS Mobile Apps periodically, at the sole discretion of the Chief Privacy Officer, to ascertain compliance with DHS privacy policy.

VII. Questions

Address any questions or concerns regarding these Instructions to the DHS Privacy Office or to the relevant Component Privacy Officer or PPOC.



Karen L. Neuman
Chief Privacy Officer

March 30, 2016

Date

Privacy Policy
For the
[INSERT NAME] Mobile Application

Overview

The overview should be a single paragraph that is used to describe the DHS Mobile Application (“DHS Mobile App”). It should include the name of the DHS component that developed the app as well as the name of the DHS Mobile App, itself. This overview should also provide a brief description of the DHS Mobile App’s purpose and function.

Information Collected

Provide the categories of individuals for whom information is collected, and for each category, list all information, including PII, SPII, and Sensitive Content that is collected by the DHS Mobile App. Details regarding the retention of information collected by the DHS Mobile App should also be addressed in this section.

Uses of Information

List each use (internal and external to the Department) of the information collected or maintained by the DHS Mobile App. Provide a detailed response that states how and why the different data elements is used.

Information Sharing

Discuss the external Departmental sharing of information (e.g., DHS to FBI). External sharing encompasses sharing with other federal, state and local government, and private sector entities.

Application Security

Discuss the technical safeguards and security controls, specific to the particular DHS Mobile App, in place to protect information that is collected and/or maintained by the DHS Mobile App.

How to Access or Correct your Information

Provide information about the processes in place for users of the DHS Mobile App to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

Analytics Tools

Discuss any analytics tools that the DHS Mobile App may use. This should include a description of any information collected through these analytic capabilities.

Privacy Policy Contact Information

Provide component privacy office contact information so that users may provide feedback and/or ask questions in regards to this DHS Mobile App Privacy Policy. This contact information may include the component privacy office’s phone number, email, and mailing address.