U.S. DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

CBP DIRECTIVE NO. 3340-049B **EFFECTIVE DATE:** 01/01/2026

ORIGINATING OFFICE: OFO/NTC
SUPERSEDES: Directive 3340-049A
REVIEW DATE: 01/01/2029

BORDER SEARCH OF ELECTRONIC DEVICES

1 PURPOSE.

1.1 This Directive provides guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in electronic devices, as defined in section 3.2, 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.

1.2 These border searches are part of CBP's longstanding practice and are essential to enforcing the law at the U.S. border and protecting border security. They help detect evidence relating to terrorism and other national security matters, human and bulk cash smuggling, narcotics smuggling, firearms smuggling, contraband, and child pornography. They enable the discovery of digital contraband, such as child pornography, illicit transfer of restricted or classified information, or other export-controlled information. They can also reveal information about financial and commercial crimes, such as those relating to copyright, trademark, smuggling, transnational theft of proprietary information 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. They can also enhance critical information sharing with, and feedback from, elements of the federal government responsible for analyzing terrorist threat information. Border searches are integral to evaluating traveler statements regarding purpose of travel and intentions upon entry or exit. Searches at the border are often essential to the enforcement of immigration laws, including determinations of admissibility.

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 Criminal Investigators, and other officials authorized by CBP to perform border searches shall adhere to the policy described in this Directive and any implementing policy memoranda, musters, and/or job aids containing policy guidance.

2.3 This Directive governs border searches of electronic devices – specifically the information in electronic or digital form contained therein. This includes 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.

2.4 This Directive does not govern actions taken to determine if a device functions (e.g., turning a device on and off or activating a screen); or actions taken to determine if physical contraband is concealed within a 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; however, CBP may not rely on search incident to arrest as a legal authority to search an arrestee's electronic device. Furthermore, this Directive does not limit CBP's ability to record actions, observations, or impressions relating to border encounters and does not restrict the dissemination of information as required by applicable statutes and Executive Orders.

2.5 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). This Directive also does not govern searches of electronic logs used to comply with federal transportation safety requirements for commercial conveyances.

2.6 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.

2.7 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, or extended border should continue to be processed pursuant to Directive 3340-032 or any successor thereto.

2.8 This Directive applies to searches performed by 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 conveys an electronic device or copies of information therefrom to HSI for analysis, investigation, and disposition (with appropriate documentation), the conveyance to HSI is not limited by the terms of this Directive, and HSI policy will apply upon HSI's receipt of the device or information. When CBP is seeking assistance from HSI under 5.5.2 and 5.5.3 of this Directive, HSI may use their concurrently held border search authority. However, CBP policy will apply if the device or information are returned to CBP to continue or conclude the border search.

2.9 CBP conducts border searches in accordance with applicable statutes, regulations, and judicial authorities. Additional or different requirements may apply in certain jurisdictions to

ensure compliance with binding circuit precedent. The location where the border search is initiated determines which policy guidance applies. For questions on specific jurisdictions, contact the CBP Associate/Assistant Chief Counsel office.

2.10 Authorized officers/agents assigned to task force operations will comply with this Directive and CBP policy.

3 DEFINITIONS

3.1 **Officer**: A U.S. Customs and Border Protection Officer, Border Patrol Agent, Air and Marine Agent, Office of Professional Responsibility Criminal Investigator, 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, flash drives, SIM cards, global positioning systems, unmanned aircraft systems, vehicle infotainment systems, smart watches, mobile phones and other communication devices, cameras, music and other media players.

3.3 **Basic Search**: Any border search of an electronic device that does not qualify as an advanced search as described in section 3.4, in which an officer conducts a review or analysis of information residing in electronic or digital form on the device. A basic search may include documenting information observed on the device during the search that relates to immigration, customs, or other law enforcement actions in CBP systems.

3.4 **Advanced Search**: An advanced search is any search in which an officer connects equipment, wired or wireless, to copy and/or analyze the contents of an electronic device. Use of external equipment (including a CBP standalone computer) merely to make the contents of the device available for inspection (including, for example, to bypass a password, overcome encryption, translate content, view files contained in an external drive or other electronic device lacking a screen, or charge a device) does not constitute an advanced search. Documenting notes and observations, as noted in section 3.3, does not constitute an advanced search.

3.5 **Sanitization**: For electronic records, sanitization includes clearing, purging and destruction in compliance with CBP Office of Information Technology Information Systems Security Policies and Procedures Handbook, HB 1400-05D or any successor thereto.

3.6 **Detention/Detained**: Detention and detained refers to the exercise of temporary custody or control over an electronic device for purposes of conducting a border search.

3.7 **Retention/Retained**: When used with respect to information, retention and retained refers to CBP's maintenance of information obtained from an electronic device after the conclusion of a border search consistent with the applicable system of records notice. Retention and retained do not include the temporary maintenance of information for a period of up to twenty-one (21) days following the conclusion of a border search to review and assess whether the information should be retained as outlined in section 5.6 of this Directive.

4 AUTHORITY/REFERENCES.

4.1 Relevant authorities and references include 6 U.S.C. §§ 122, 202, 211; 8 U.S.C. §§ 1103, 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; Memorandum from Secretary Janet Napolitano, *The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities* (April 26, 2013); Memorandum from Acting Secretary Kevin K. McAleenan, *Information Regarding First Amendment Protected Activities* (May 17, 2019).

4.2 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." *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. Odutayo*, 406 F.3d 386, 391-92 (5th Cir. 2005); *United States v. Boumelhem*, 339 F.3d 414, 422-23 (6th Cir. 2003); *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).

4.3 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 authority. *See Boumelhem*, 339 F.3d at 423.

4.4 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.

4.5 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 and disabling Bluetooth and Wi-Fi connections) 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 An officer may conduct a basic search of an electronic device with or without suspicion, subject to the requirements and limitations provided herein and applicable law.

5.1.4 An officer may perform an advanced search of an electronic device only in instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP or, in the absence of individualized reasonable suspicion when there is a national security concern. All advanced searches require supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities). In cases where the inspecting officer and

approving supervisor rely on the presence of a national security concern, without reasonable suspicion, to conduct an advanced search, approval from the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or their delegate, is required prior to conducting the search. In compelling circumstances where operational considerations prevent prior approval, notification shall be made as soon as possible. Notification must include an explanation of the national security concern, the compelling circumstances that precluded prior approval, the relevant facts and information supporting the search, and the results of the search.

5.1.5 All searches of electronic devices will be documented in appropriate CBP systems. Officers will document any supervisory approvals required under this Directive and, in the case of an advanced search, the factors establishing reasonable suspicion of a violation of a law enforced or administered by CBP or a national security concern, as well as relevant observations, impressions, and actions taken, as appropriate.

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.

5.1.7 Notification of Border Search

Prior to the initiation of the border search of the electronic device, the individual will be notified of the purpose and authority for such search, how the individual may obtain more information on reporting concerns about the search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search. Officers may distribute an approved tear sheet, if available, to provide this notification, as appropriate. If the officer, or other appropriate CBP official, determines that the fact of conducting the search cannot be disclosed without impairing national security, law enforcement, officer safety, or other operational interests, notification may be withheld with approval from the appropriate supervisor. Officers must document in appropriate CBP systems the method by which the notification was provided to the traveler or state the reason why it was not provided.

5.1.8 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 Privacy Officer and to the Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or equivalent level manager.

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 engage with the U.S. Attorney's Office as needed, officers will segregate any privileged material from other information examined during a border search to ensure that any privileged material is handled appropriately while also safeguarding CBP's 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 responsible CBP Associate/Assistant Chief Counsel office. Use of external equipment to copy the contents of a device solely to segregate privileged material from non-privileged material, to conduct a Filter Team review, or to otherwise implement the requirements of section 5.2.1.2 or 5.2.1.3 does not convert a basic search into an advanced search.

5.2.1.3 Unless an imminent threat to life or to homeland security is identified therein, copies of the materials maintained by CBP and determined to be privileged will be sanitized at the completion of CBP's review. This excludes 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, the Privacy Act, and any applicable system of records notice.

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 that is protected by a passcode, 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 maintained for the duration of the search if 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 or other means of access obtained during a border inspection will only be utilized to facilitate the inspection of devices and information subject to border search. Passcodes or other means of access may not be utilized to access information that is only stored remotely. Passcodes or other means of access should only be recorded by the officer in a temporary format and should not be uploaded into CBP systems. Passcodes or other means of access recorded by the officer will be deleted or destroyed when no longer needed to facilitate the search of a given device.

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

5.4 Detention of an Electronic Device in Continuation of a Border Search

5.4.1 Detention for Continuation of a Border Search
An officer may detain electronic devices 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. 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, 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 for continuation of a border search after an individual's departure from the port or other location of a CBP encounter. Unless extenuating circumstances exist, the detention of devices ordinarily should not exceed five (5) calendar days. Detention of an electronic device may be extended beyond five (5) calendar days with the approval of a Port Director; Patrol Agent in Charge; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or other equivalent level manager. Extensions of detentions exceeding fifteen (15) calendar days may be approved and re-approved in increments of no more than seven (7) calendar days by the Director, Field Operations; Chief Patrol Agent; Director, Air Operations; Director, Marine Operations; Special Agent in Charge; or their delegate. Approvals for detention and any extension thereof shall be noted in appropriate CBP systems. The requirements in this section also apply to devices conveyed to another agency or entity for assistance during the border search, as detailed in section 5.5.

5.4.1.2 Custody Receipt
If CBP determines it is necessary to temporarily detain an electronic device to continue the search, the officer detaining the device shall issue a completed Form 6051D to the individual. All transfers of the custody of the electronic device will be recorded on the Form 6051D, including transfers to HSI as noted in section 2.8. The Form 6051D shall be uploaded as an attachment in the documentation of the search in the appropriate CBP system upon initial issuance and upon final disposition of the device.

5.5 Requests for Assistance in Support of a Border Search of an Electronic Device

5.5.1 Procedures and Requirements when Seeking Assistance
Officers may request assistance to facilitate access to and search of an electronic device and the information stored therein. 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. 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. Requests for assistance require supervisory approval and shall be properly documented and recorded in CBP systems. Detentions executed to seek assistance must comply with section 5.4.

5.5.1.1 Electronic devices should be transferred only when necessary to render the requested assistance. Otherwise, a copy of the information from the device should be conveyed in lieu of the electronic device itself.

5.5.1.2 When an electronic device or information contained therein is conveyed outside of CBP 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 Form 6051D.

5.5.2 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. Technical assistance may also be required if initial efforts to access or copy the information on the device are unsuccessful. 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 with or without suspicion, subject to the requirements and limitations provided herein and applicable law.

5.5.3 Subject Matter Assistance – With Reasonable Suspicion

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 they have reasonable suspicion of activities in violation of the laws enforced or administered by CBP. Where subject matter assistance is requested, responses should include all appropriate findings, observations, and conclusions relating to the laws enforced or administered by CBP.

5.5.4 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 request 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 5.5.6. 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.

5.5.5 Disposition Following Assistance

CBP will request that at the conclusion of the requested assistance, all information be returned to CBP as expeditiously as possible. In addition, the assisting agency or entity should sanitize all copies of the information conveyed unless section 5.5.6 applies. In the event that any electronic devices are conveyed, consistent with section 5.1.2, actions must not be taken that would make any changes to the contents of the device. The device and all copies of information are to be returned to CBP unless seized by an assisting agency based on probable cause or retained per 5.5.6.

5.5.6 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 of information from devices 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. In the event that an assisting federal agency has independent authority to retain the device, the assisting federal agency will coordinate with CBP.

5.6 Retention of Information Discovered in the Border Search of an Electronic Device

5.6.1 Retention of Information with Probable Cause
CBP may retain copies of information from an electronic device when, based on a review of the information encountered or on other facts and circumstances, they determine there is probable cause to believe the information contains digital contraband or evidence of a violation of law that CBP is authorized to enforce or administer, subject to the requirements and limitations provided herein and applicable law.

5.6.2 Retention of Information in CBP Privacy Act-Compliant Systems
Without probable cause, CBP may retain only information from the border search of an electronic device relating to immigration, customs, and other enforcement matters if such retention is consistent with the applicable system of records notice and subject to the requirements and limitations provided herein and applicable law.

5.6.3 Retention Consistent with Discovery Obligations
Notwithstanding sections 5.6.1 and 5.6.2, there may be instances when, in consultation with the Office of Chief Counsel, it is determined that the information should be retained consistent with discovery obligations in ongoing or reasonably anticipated litigation. In such instances, retention procedures, including the appropriate method for storage, will be determined on a case-by-case basis.

5.6.4 Timeframe for Retention Determination
Following the completion of the border search, CBP will retain no copies of the information beyond twenty-one (21) calendar days following the conclusion of the border search unless retention is permissible or required consistent with sections 5.6.1, 5.6.2, or 5.6.3.

5.7 Seizure of an Electronic Device Resulting from a Border Search

5.7.1 Officers may seize an electronic 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-contains digital contraband or evidence of a violation of law that CBP is authorized to enforce or administer.

5.8 Sharing of Information Obtained from Border Searches of Electronic Devices

5.8.1 Sharing Generally
CBP is authorized to share copies of information contained in electronic devices (or portions thereof), which are retained in accordance with this Directive, with federal, state, local, tribal,

territorial, and foreign law enforcement agencies, in compliance with applicable law and policy related to information sharing for law enforcement and security purposes. Nothing in this Directive limits this authority.

5.8.2 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 or administered 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.

5.9 Reporting Requirements

5.9.1 The officer performing the border search of an electronic device 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, maintenance, 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, as detailed in section 5.1.5.

5.9.2 In instances where an electronic device or copy of information contained therein is conveyed within CBP the receiving officer is responsible, in coordination with the initiating office as necessary, for ensuring all information related to the search from the point of receipt forward through the final disposition is recorded.

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

5.10 Management Requirements

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

5.10.2 The appropriate CBP second-line supervisor shall monitor the status of the detention of all electronic devices and ensure any required extensions are submitted for executive review and documented appropriately.

5.10.3 The appropriate CBP second-line supervisor shall 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 and ensure all appropriate actions are taken and documented.

5.10.4 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 and retention of information contained therein in order to ensure compliance with the procedures outlined in this Directive.

5.10.5 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.

6.1 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.

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

8 NO PRIVATE RIGHT CREATED.

8.1 This Directive is an internal policy statement of CBP and does not create or confer any rights, privileges, or benefits on any person or party.

9 REVIEW.

9.1 This Directive shall be reviewed at least every three years and updated as necessary.

10 DISCLOSURE.

10.1 This Directive may be shared with the public.

11 SUPERSEDES.

11.1 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. 3340-049A, Border Search of Electronic Devices (January 4, 2018).

Rodney S. Scott
Commissioner