



Border Search of Electronic Devices at Ports of Entry

U.S. Customs and Border Protection (CBP) is responsible for protecting our nation's borders and enforcing numerous laws at U.S. ports of entry. CBP's ability to lawfully inspect electronic devices crossing the border is integral to keeping America safe in an increasingly digital world.

All travelers crossing the United States border are subject to CBP inspection. On rare occasions, CBP officers may search a traveler's mobile phone, computer, camera, or other electronic devices during the inspection process. These searches have been used to identify and combat terrorist activity, child pornography, drug smuggling, human smuggling, bulk cash smuggling, human trafficking, export control violations, intellectual property rights violations and visa fraud, among other violations. Furthermore, border searches of electronic devices are often integral to determining an individual's intentions upon entry to the United States and thus provide additional information relevant to admissibility of foreign nationals under U.S. immigration laws.

CBP has established strict guidelines, above and beyond prevailing legal requirements, to ensure that these searches are exercised judiciously and responsibly and are consistent with the public trust.

The number of travelers crossing the border that experience a border search of their electronic devices is small. In Fiscal Year (FY) 2024, **less than 0.01 percent** of arriving international travelers encountered by CBP at a port of entry had their electronic devices searched. Additional statistics are available in the Frequently Asked Questions below and Relevant Policies and Documents box to the right of this page.

General Information

 [Close all](#)  [Open all](#)

What is a border search of electronic device? —

Border searches of electronic devices have long been critical to protecting border security, and are essential to enforcing the customs, immigration, and other laws CBP is authorized to enforce and administer. Border searches of electronic devices include any inbound or outbound search pursuant to longstanding border search authority and are conducted at the physical border, the functional equivalent of the border, or the extended border, consistent with law and agency policy.

What is the authority for CBP to search electronic devices? —

CBP conducts border searches of electronic devices in accordance with statutory and regulatory authorities, as well as applicable judicial precedent, including United States Supreme Court precedent recognizing the authority of the government to conduct border searches. All persons regardless of citizenship, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection by CBP. CBP's border authorities permit the inspection, examination, and search of vehicles, persons, baggage, and merchandise to ensure compliance with the laws enforced or administered by CBP. This search authority extends to electronic devices crossing our nation's borders.

Border searches are an integral aspect of CBP's border security and counterterrorism responsibilities under Title 6 of the U.S. Code, enforcement of laws relating to customs and international trade under Title 19 of the U.S. Code, and enforcement of the immigration laws under Title 8 of the U.S. Code, in addition to numerous other federal laws that CBP enforces and administers at the border.

For what purpose does CBP conduct border searches of electronic devices? —

Border searches of electronic devices are conducted by CBP to enforce the law at the U.S. border and to protect border security, in accordance with statutory and regulatory authorities, as well as applicable judicial precedent. This includes

ATLA Doc. No. 24121202. (Posted 12/12/24)

determining whether a device contains digital contraband (e.g., child pornography, classified materials, export-controlled information), terrorism-related information, or information relevant to a visitor's admissibility or otherwise relevant to enforcement of the Immigration and Nationality Act. As permissible, border searches may also help detect other national security matters, as well as reveal information about transnational financial crimes, including bulk cash smuggling, and commercial crimes with a nexus to the border, such as those relating to copyright and trademark.

What types of border searches does CBP conduct?

CBP [policy](#) distinguishes between a “basic” and an “advanced” search.

A *basic search* is any border search of an electronic device that is not an advanced search, as described below. A basic search generally entails an officer reviewing the contents of the device manually without the assistance of any external equipment.

An *advanced search* is any search in which an officer connects external equipment to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents. Under CBP policy, advanced searches require reasonable suspicion of a violation of law enforced or administered by CBP or a national security concern and require the approval of a senior manager (at a Grade 14 level or higher, or a manager with comparable responsibilities) prior to conducting the search.

How many border searches of electronic devices has CBP conducted?

Despite the fact that all merchandise and persons crossing the border, both inbound and outbound, are subject to inspection by CBP, the number of travelers crossing the border whose electronic devices are actually searched is small. In FY 2024, out of the over 420 million travelers CBP processed at ports of entry, CBP only searched the electronic devices of 47,047 international travelers.

Upon arrival in the United States, travelers regardless of citizenship are generally required to present themselves for inspection at the port of entry’s primary arrival location, often referred to as “primary” or “primary inspection.” At primary, CBP officers generally inspect all travelers seeking entry to the United States to determine their identity, their citizenship, their eligibility to enter the United States, whether any merchandise in their custody or control is prohibited or subject to duty, and to identify violations of law that CBP enforces or administers. Travelers whose processing may take more than a few moments or who may warrant extra scrutiny may be referred for further inspection, often referred to as “secondary” or “secondary inspection.” Officers at primary inspection have broad discretion to refer travelers for secondary inspection, with or without any suspicion of wrongdoing. Some reasons that a traveler may be referred for secondary inspection include (1) to address issues with the documentation or information supplied by the traveler; (2) to address potential administrative immigration violations; (3) to conduct inquiries regarding potential violation of civil or criminal laws enforced or administered by CBP; (4) to screen at random; (5) if CBP officers at primary inspection believe, at their discretion, that further inspection is needed; or (6) if CBP officers at primary inspection are alerted to an issue that may require further inspection. At the secondary inspection location, CBP officers will conduct further assessment to resolve the reason for the referral. Of the 420 million travelers CBP processed at ports of entry in FY 2024, 12,660,784 (3%) travelers were referred for a secondary inspection.

A border search of electronics is **not** a required action during a secondary inspection. In fact, CBP only conducted border searches of the electronic devices of 47,047 travelers in FY 2024, representing approximately 0.3% of secondary inspections and less than 0.01% of all arriving international travelers encountered at ports of entry.

Of the 47,047 border searches of electronic devices encountered at port of entry, 42,725 (90%) were basic searches in which the devices were not connected to external equipment to review, copy and/or analyze its contents.

International Travelers Processed with Electronic Device Search*

Fiscal Year Quarter	Total Border Searches Conducted	Total Basic Searches Conducted	Total Advanced Searches Conducted
FY 24, Q1	10,937	9,883	1,054

Fiscal Year Quarter	Total Border Searches Conducted	Total Basic Searches Conducted	Total Advanced Searches Conducted
FY 24, Q2	11,273	10,250	1,023
FY24, Q3	12,090	11,082	1,008
FY24, Q4	12,658	11,504	1,154

Historical statistics are available on the [CBP Enforcement Statistics](#) webpage.

** Statistics may vary from previously reported monthly statistics as a result of reporting that is finalized after CBP initially retrieved the statistics from our live systems for the monthly reporting.*

Am I obligated to provide my electronic device(s) and associated password(s) to CBP? —

Pursuant to CBP's border search authority explained above, when presenting their effects for inspection, all travelers are obligated to present their electronic devices and the information resident on the device in a condition that allows for the examination of the device and its contents. If the electronic device cannot be inspected because it is protected by a passcode or encryption or other security mechanism, that device may be subject to exclusion, detention, or other appropriate action or disposition. Additionally, the traveler may face longer processing times to allow for CBP to access the contents of the device.

Foreign nationals who are applicants for admission to the United States must establish to the satisfaction of the inspecting CBP officer that they are entitled to enter the United States. Admissibility determinations are made based on the totality of the circumstances. If a foreign national refuses to present their electronic devices and the information resident on the device in a condition that allows for the examination of the device and its contents, CBP may consider the foreign national's noncompliance and the inability to inspect the device when making admissibility decisions and

may take appropriate law enforcement actions. However, CBP's ability to inspect an electronic device alone does not determine admissibility.

If a traveler being admitted as a U.S. citizen does not present their device in a condition that allows for examination, the U.S. citizen traveler will not be denied entry into the United States based on CBP's inability to complete an inspection of their device. However, as noted above, their device may be subject to exclusion, detention, or other appropriate action or disposition.

Any passcodes or other means of access provided by the traveler will be used as needed to facilitate the examination; however, they will 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.

Data Use and Retention

Does CBP document when border searches of electronic devices are conducted? —

CBP documents relevant information regarding border inspections, including inspections of both basic and advanced searches, in its primary law enforcement system, TECS.

CBP officers document border 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.

For a complete overview of TECS, its functions, and the associated privacy risks, visit www.dhs.gov/privacy-impact-assessments. Click on "**CBP**" at the left and then "[DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing](#)" and "[DHS/CBP/PIA-021 TECS System: Platform](#)".

Does CBP retain information from border searches of electronic devices? —

Pursuant to the [CBP Directive](#), CBP may retain copies of information obtained from a border search of an electronic device after the conclusion of the search: (1) if there is probable cause to believe the information contains evidence of a violation of law that CBP is authorized to enforce or administer, or (2) if the information relates to immigration, customs, or other enforcement matters.

Any retention is consistent with applicable [system of records notices](#), as well as CBP privacy and data protection standards. For information retained following a border search of an electronic device encountered at a port of entry, the information may be retained in CBP's Automated Targeting System (ATS) for a period not to exceed 15 years, after which time the records will be deleted. If the record is linked to an active law enforcement lookout record, CBP matches to enforcement activities, or active investigations, the information will remain accessible for the life of the law enforcement activity. Safeguards are employed to govern access to and use of the data.

Where is the data retained? —

Information retained following a border search of an electronic device encountered at a port of entry is retained in ATS which has robust access controls limiting user access to only those with a need to know. Any further retention of data and sharing of data obtained from border searches of electronic devices are conducted in compliance with the CBP System of Record Notice for ATS.

More information is available at www.dhs.gov/privacy-impact-assessments. Click on “**CBP**” at the left and then “[DHS/CBP-PIA-006 Automated Targeting System](#)”.

Will my information be made available outside the Department of Homeland Security? —

The information obtained during the course of a border search may be made available to other agencies, or subject matter experts, if CBP determines there is a need for further investigation, to obtain assistance such as subject matter expertise, translation assistance, decryption, or other technical assistance; or the disclosure is consistent with the Privacy Act and CBP privacy and data protection standards. As a federal law enforcement agency, CBP may generally share lawfully maintained information with other federal, state, local, and foreign law enforcement agencies for law enforcement purposes, consistent with the routine uses contained in the applicable system of records notices.

Privacy and Transparency

Does CBP have policies and procedures for initiating border searches of electronic devices? —

CBP's policies and procedures for initiating border searches of electronic devices are outlined within [CBP Directive No. 3340-049A, Border Search of Electronic Devices](#). As a policy matter, CBP has imposed certain requirements, above and beyond prevailing constitutional and legal requirements, to ensure the authority for border search of electronic devices is exercised judiciously, responsibly, and is consistent with the public trust. CBP regularly conducts reviews of its policies and procedures to ensure an appropriate balance between privacy protections and operational mission requirements.

What privacy protections does CBP have in place to safeguard the public's information? —

CBP works diligently to ensure that privacy protections are balanced against its national security and border enforcement missions and remains committed to providing as much notice and transparency regarding its border searches of electronic devices as possible.

ATS users must undergo annual security and data privacy training and obtain approval from CBP management and the ATS system owner before gaining access to ATS for official purposes. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Further, search activities in ATS are recorded for all users and fully auditable. Access to information in ATS from the border search of an electronic device is further restricted by user profiles to those CBP personnel who have a need-to-know the information for their official government duties.

CBP also works closely with privacy offices within the agency and DHS to ensure compliance with all legal and policy privacy requirements. More information is available at www.dhs.gov/privacy-impact-assessments. Click on “**CBP**” at the left and then “[DHS/CBP-PIA-008 Border Searches of Electronic Devices](#)”.

Does CBP search information that is stored remotely (in the cloud)?

The border search will only include an examination of information that is resident upon the device at the time it is presented for inspection. CBP officers may not use the device to access information that is solely stored remotely.

Prior to beginning a basic or advanced search, CBP Officers will ensure all data and network connections are disabled. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, CBP Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode, disabling Bluetooth and disabling Wi-Fi), or the CBP Officer will themselves disable network connectivity.

Does CBP provide notice to the traveler regarding the border search of electronics?

CBP provides signage in inspection areas that vehicles and other conveyances, persons, baggage, packages, or other containers are subject to detention and search. Additionally, CBP posts information on cbp.gov regarding border searches of electronic devices.

CBP has also created [tear sheets](#) to provide travelers information regarding the search of their electronic devices. The tear sheet notifies 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 they feel aggrieved by a search.

Last Modified: Nov 20, 2024

Relevant Policies and Documents

[CBP Border Search of Electronic Device Directive](#)

[Border Search of Electronic Devices Tear Sheet](#)

[FY23 Annual Statistics](#)

[FY24 Annual Statistics](#)