# Privacy Impact Assessment

**for the**

# U.S. Border Patrol Digital Forensics Programs

**DHS Reference No. DHS/CBP/PIA-053(a)**

**July 30, 2020**

Homeland Security

# Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), U.S. Border Patrol (USBP) conducts searches of electronic devices to identify violations of the laws CBP enforces and administers, including laws relating to the detection and apprehension of illicit goods and individuals entering and exiting the United States in between ports of entry (POE). Depending on the circumstances, CBP conducts searches of electronic devices pursuant to different legal authorities. CBP is publishing this Privacy Impact Assessment (PIA) update to analyze the privacy risks of expanded digital forensic tools and an enterprise-wide solution for managing and analyzing certain types of metadata that USBP collects from electronic devices across its digital forensic collection activities. In addition, this updated PIA will clarify that searches may be conducted pursuant to border search authority.

# Overview

CBP is responsible for securing the borders of the United States while facilitating lawful international trade and travel. CBP employs various technologies to enforce and administer hundreds of U.S. laws and regulations at the border, including immigration and narcotics enforcement laws. CBP enforces compliance with numerous federal laws at the border to prevent contraband, other illegal and restricted merchandise, and inadmissible persons from entering and exiting the United States. CBP enforces these laws both at and between POE.

USBP Agents work to detect, identify, interdict, and apprehend individuals with ties to terrorism, as well as individuals conducting smuggling activities involving: humans, narcotics, weapons, bulk cash, and other prohibited or restricted merchandise. USBP Agents may encounter and collect information and evidence from a variety of sources during an interdiction. As part of USBP's law enforcement duties, USBP may search and extract information from electronic devices, including: laptop computers; thumb drives; compact disks; digital versatile disks (DVDs); mobile phones; subscriber identity module (SIM) cards; digital cameras; vehicles; and other devices capable of storing electronic information.[1]

USBP Agents may search electronic devices in a variety of scenarios, including:

- **Border Search.** All travelers and the items they carry, including electronic devices, are subject to search by CBP when crossing the U.S. border (inbound/outbound) at or between POEs, at the functional equivalent of the border, and at the extended border. CBP is authorized to conduct these searches to enforce immigration, customs, and other federal laws at the border. CBP provides additional notice and a thorough discussion

[1] Unlike searches performed pursuant to CBP policy for border searches of electronic devices, in certain circumstances, USBP may access information from the cloud if the search of the electronic device is conducted pursuant to a warrant or consent. If cloud-based information is not specifically mentioned in the warrant, then USBP would not extract data from the cloud.

of border searches of electronic devices in a PIA published in January 2018.[2]

- **Warrant Search.** Warrants issued by a judge or magistrate may authorize CBP to search electronic devices. Such searches generally occur in furtherance of a criminal investigation, subsequent to a finding of probable cause by a judge or magistrate.
- **Consent Search.** Owners/possessors of a device may authorize CBP to search the electronic device. USBP generally conducts consent searches in situations in which they believe that the device may contain information relevant to a law enforced or administered by CBP. For consent searches, CBP generally requires written consent from the owner or individual in possession of the device. All consent must be voluntarily given, depending on the totality of the circumstances. To the extent that CBP has encountered individuals who do not speak English, CBP will follow all applicable language access policies.[3] In the event that an individual declines to provide his or her consent, CBP may pursue a warrant authorizing a search of the device or determine if other legal options apply.
- **Abandonment Search.** CBP Officers and Agents regularly encounter abandoned property,[4] including electronic devices. In some cases, CBP may suspect that the unclaimed property may be associated with a criminal act, whereas in others, CBP Officers and Agents may find an abandoned device under unusual circumstances (such as between POEs in close proximity to the border). CBP may retrieve and search abandoned devices without any level of suspicion required.
- **Exigent Circumstances Search.** In the extremely rare circumstances in which they exist, exigent circumstances may permit an Agent to conduct a warrantless search of an electronic device if he/she has probable cause and the exigent circumstances require immediate action. Exigent circumstances may justify a warrantless search of an electronic device if there is a true "now or never" situation involving the need to prevent the imminent destruction or loss of evidence, or if there is an imminent threat to the

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE BORDER SEARCHES OF ELECTRONIC DEVICES, DHS/CBP/PIA-008(A) (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[3] It is the policy of CBP to make reasonable efforts to provide meaningful access, free of charge, to persons with limited English proficiency to its operations, services, and other conducted activities and programs without unduly burdening the Agency's fundamental mission. This obligation applies to any medium of communication and to interactions with the public, including but not limited to, in-person or telephonic contact; written correspondence, including email; use of websites and newsletters; community engagement events and activities; and documents explaining CBP programs. *See* U.S. CUSTOMS AND BORDER PROTECTION, LANGUAGE ACCESS, https://www.cbp.gov/about/language-access (last visited July 28, 2020).

[4] Generally, abandoned property in this context refers to personal property that a CBP Officer or Agent finds in the field or at the scene of a law enforcement action, and the individuals present disavow ownership of the property.

safety of the public or law enforcement, such as a life or death situation. USBP will coordinate with counsel before searching a device pursuant to exigent circumstances.

When USBP encounters an electronic device pursuant to one of these scenarios, the USBP Agent may submit the electronic device for digital forensic analysis in accordance with applicable law and policy. USBP Sector Intelligence Units, which are staffed with dedicated CBP personnel who are trained to conduct forensic analysis of electronic devices obtained pursuant to USBP's authorities, are responsible for conducting digital forensics investigation. In the event the USBP Sector does not have the appropriately trained personnel, the USBP Sector will store the electronic device consistent with CBP evidence handling procedures and request that the CBP Laboratories and Scientific Services Directorate (LSSD) provide technical assistance and analysis.[5]

CBP conducts searches to identify contraband or evidence relevant to the laws enforced or administered by CBP. If, during a search, CBP comes across evidence of violations of law within the purview of another law enforcement agency, CBP may contact the appropriate DHS or external partner for appropriate action. CBP personnel trained to extract data from electronic media work with the USBP case Agent to determine what information is pertinent to the investigation. The USBP case Agent then reviews all the information to assess whether there is relevant information that is within the scope of USBP's legal authority. Any information obtained through a search warrant and found to be non-responsive to the scope of the warrant will be removed and permanently deleted from the system in its entirety upon conclusion of the case or trial, after approval from the U.S. Attorney or relevant prosecutor's office.

## Reason for the PIA Update

CBP is updating the previously issued USBP Digital Forensics PIA to document changes since the original PIA was published in April 2018. Specifically, this PIA discusses CBP's development of enterprise-wide solution to manage and analyze certain types of information and metadata USBP collects from electronic devices. CBP uses various technical tools and software applications to retain, analyze, and manage information collected from electronic devices pursuant to applicable legal authorities. These tools do not change how CBP stores information in its IT systems or the process USBP Agents must go through to request a digital examination. Additionally, this PIA clarifies that USBP conducts forensic examinations under CBP's border

[5] The LSSD operates the seven nationally-accredited CBP Field Laboratories, numerous satellite laboratories at CBP's front line, the Methods Development/Special Projects laboratory, the 24/7 Teleforensic Center, the Interdiction Technology Branch, as well as a Headquarters location for administrative management and CBP-wide scientific services functions. LSSD technical staff are badged, law-enforcement forensic scientists and engineers. LSSD performs scientific analysis, renders technical reports and opinions, and executes broad forensic capabilities, including crime scene and use-of-force investigations, in support of CBP's core mission. In addition, LSSD administers CBP's Commercial Gauger and Laboratory Approval and Accreditation Program and National Weights and Scales program, verifies the technical acceptability of narcotics destruction facilities, provides 24/7 teleforensic support and technical advice to field personnel for suspect weapons of mass destruction, detection events, and coordinates expertise in interdiction and applied enforcement technologies.

search authority, in addition to searches conducted pursuant to warrant, consent, and abandonment.

**Border Search Authority**

USBP border searches of electronic devices are governed by a CBP Directive[6] and the process is explained in the previously published Border Searches of Electronic Devices PIA.[7] Any changes to the CBP Directive or CBP's use of border search authority to conduct searches of electronic devices will be documented in the Border Searches of Electronic Devices PIA. The primary purpose of this (USBP Digital Forensics) PIA is to document the tools and processes USBP uses to conduct digital forensics on electronic devices, regardless of the authority under which the exams occur.

**USBP Enterprise Solutions for Digital Forensics**

USBP collects information from electronic devices detained or seized pursuant to one of the above-mentioned search authorities. The local USBP Sector-based Evidence Collection Team or a trained USBP Agent or analyst of a Sector Intelligence Unit conducts the digital forensic processing on the electronic device, in coordination with the USBP case Agent who detained or seized the electronic device. USBP uses various digital forensic extraction tools to acquire a mirror copy of the data on the device. As described in the previous PIA, digital forensic tools enable CBP to conduct a variety of analyses on electronic device data, including: 1) timeframe analysis, which can help in determining when data was entered, modified, or deleted from a device; 2) detection and recovery of concealed data; 3) correlation of files to installed applications, examination of drive file structure, and review of metadata; and 4) reviews to help to identify individuals who created, modified, or accessed a file.

Digital forensic tools have varying levels of functionality, but at a minimum all of these tools can perform the following functions:

- The capability to extract or acquire an exact image copy (this can be a logical image[8] or a physical image[9]);

---

[6] *See* U.S. CUSTOMS AND BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES (2018), *available at* https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

[7] *See supra* note 2.

[8] A logical forensic image is a static capture or snapshot of the contents of a partition or drive at a specific moment in time. A logical forensic image of a hard drive contains all of the "active" data, which generally refers to data a user wants to see, or needs to see, and is formatted within a file system. If a forensic examiner creates a logical forensic image of a 1 terabyte (TB) drive, the logical image will only contain a portion of the 1 TB drive. The typical data available via a logical image extraction are call logs, Short Messaging Service (SMS), commonly known as text messages, Multimedia Messaging Service (MMS), which are generally text messages with attachments or group text messages, images, videos, audio files, contacts, calendars and application data.

[9] Physical forensic image is a static capture or snapshot of the contents of a partition or drive at a specific moment in time. A physical image is a bit-by-bit copy from the first sector to the last sector of a storage media which includes the user-addressable sectors composed of allocated and unallocated space. This type of extraction allows for the

- The ability to read and analyze the extracted image copy (e.g., logical or physical analyzer); and
- The ability for the tool to isolate key metadata and produce a read-only report of relevant data that PenLink (explained below) can ingest.

Trained and authorized USBP personnel use digital forensic tools to initially exploit electronic media. These tools enable USBP personnel to rapidly access and extract file system data from the electronic device. The digital forensic tools communicate directly with the operating system of the electronic device and extract all system and deleted data out of the electronic device. When authorized by a search warrant, a digital forensic tool may be used to overcome security and encryption challenges on a locked electronic device.

**PenLink (PLX)**

USBP stores the images and copies taken from an electronic device via digital forensic tools in a standalone Local Digital Forensic Network (LDFN) located at each USBP Sector HQ or Station. USBP cannot upload the raw extracted data from electronic devices directly to the CBP network due to potential security violations (e.g., the extracted data may include pornographic images). Therefore, USBP will save the initial extracted information in a LDFN to verify whether any of the data is unsuitable for the CBP network. If the data is "clean," trained USBP personnel will transfer the data to PLX, the USBP-wide solution for managing extracted digital forensic metadata. USBP will only store the image copy extracted from an electronic device on the LDFN.

USBP uses PLX to ingest the metadata from the forensic acquisition report, which is a report created from the image copy by a digital forensic tool. As explained above, USBP stores the initial extraction on a standalone LDFN for further analysis using ADACS4[10] or similar system. USBP Agents then determine what relevant information to transfer onto CBP servers. USBP transfers the forensic acquisition report (in either xml, pdf, or csv file format) from the LDFN to a CBP-approved encrypted thumb drive. USBP then transfers the data on the thumb drive to a CBP networked computer running PLX. During the upload process to PLX, the USBP Agent or CBP digital forensic examiner will assign a case number which will later be used to link the extracted data to the corresponding case in the sector's local case management system.

USBP will use PLX to address the lack of an enterprise system of record for its digital forensic collection activities that is able to link data extractions across USBP use cases. USBP will use triage procedures based on best practices developed by the CBP LSSD to determine what type of data should be transferred to PLX and what process to follow. In general, videos will not be forensically extracted for collection and analysis unless the USBP Agent determines relevant data

collection of all live data and also recovery of data that has been deleted or is hidden.

[10] ADACS4 is an IT system used to analyze data from electronic devices to discover connections, patterns, and trends related to terrorism, human and narcotic smuggling, and other activities posing as a threat to border security.

exists during the basic search of the device.[11] If a USBP Agent suspects prohibited material (such as child pornography) is contained on the electronic device, the forensic case processing will be referred to U.S. Immigration and Customs Enforcement, Homeland Security Investigations.

By using PLX, USBP will standardize the way it collects, retains, and uses information derived from digital forensic cases and data obtained from telecommunications providers pursuant to subpoenas or warrants. PLX follows standard procedures for maintaining evidence. Initial implementation will occur at select USBP Sectors with the plan to rollout PLX as USBP's enterprise-wide solution and system of record.

Information USBP may extract or later identify and retain from an electronic device may include the following:

- Contacts;
- Call Logs/Details;
- IP Addresses used by the device;
- Calendar Events;
- GPS Locations used by the device;
- Emails;
- Social Media Information;
- Cell Site Information;
- Phone Numbers;
- Videos and Pictures;
- Account Information (User Names and Aliases);
- Text/chat messages;
- Financial Accounts and Transactions;
- Location History;
- Browser bookmarks;
- Notes;
- Network Information; and
- Tasks List.

These files may contain text that includes biographic and other information related to the owner of the device and any contacts.

[11] *See supra* note 2.

# Privacy Impact Analysis

### Authorities and Other Requirements

CBP authorities for collecting and retaining information from electronic devices have not changed. CBP and USBP have issued some additional guidance documents setting out policies for how USBP can conduct border searches of electronic devices, including for example:

- USBP Digital Forensics/Document and Media Exploitation IOP 3340-049;
- CBP Directive No. 3340-049A; Border Searches of Electronic Devices, (01/04/2018) and related memos and musters; and
- DHS/CBP/PIA-008(a) Border Searches of Electronic Devices (January 4, 2018).

### Characterization of the Information

There is no change to the information USBP collects, uses, disseminates, or maintains as a result of this PIA update.

### Uses of the Information

The PLX system is a new capability that USBP is using to access, identify, and store information found during digital forensic exams. There is no change to how USBP uses the information it views and retrieves during digital forensic exams. USBP uses the information it gathers using these tools to develop leads, identify trends associated with illicit activity, and further law enforcement actions related to terrorism, human and narcotic smuggling, and other activities posing a threat to border security or national security or indicative of criminal activity. USBP may also conduct border searches of electronic devices of devices that are in the possession of aliens crossing the border between the POEs.

**Privacy Risk:** With the new capability to store and search extracted information from devices at an enterprise-level, there is a risk that irrelevant information extracted from devices will now by accessible to a larger number of USBP agents with no nexus to that particular case.

**Mitigation:** This risk is mitigated. CBP has restricted access to the digital forensic tools and PLX system. Only trained forensics technicians will have access to the digital forensic tools. The forensic technician will work with the case agent to determine what information is relevant. All extracted data will be maintained on the LFDN, only a limited number of personnel with an operational need will have access to the LFDN, and only relevant data will be transferred to PLX. All CBP personnel are required to complete the Annual DHS Privacy Training and CBP IT Systems Security Training.

### Notice

There is no change to how USBP provides individual notice regarding the search, retention, and seizure of electronic devices or copies of information extracted from electronic devices. This PIA update and the Border Searches of Electronic Devices PIA published in 2018 provide notice to the public of CBP's search, retention, and analysis of information contained in electronic devices. USBP may ask an individual for consent before searching an electronic device, or may conduct searches pursuant to other authorities, as explained above. In some cases, asking for consent in addition to searching the device in the presence of an individual provides additional notice to individuals about USBP actions. In cases where USBP Agents detain or seize electronic devices, the USBP Agent will provide a tear sheet to individuals notifying them of USBP actions.

**Privacy Risk:** There is a risk that individuals do not have notice that USBP may search their electronic devices and conduct forensic examination as part of a border search.

**Mitigation:** This risk is mitigated. CBP has provided notice and transparency about its digital forensic program and border search authority by publicly releasing the policy[12] for these searches and publishing this and corresponding PIAs.[13]

When possible, USBP conducts searches of electronic devices 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 during the search of the device. Permitting an individual to remain present during a search does not necessarily mean that the individual shall observe the search. If permitting an individual to observe the search could reveal law enforcement techniques or potentially compromise operations, the individual will not be permitted to observe the search of the device.

### Data Retention by the Project

There is no change to how long USBP retains records of arrest, detentions, removals, and associated information (such as information obtained from electronic devices) for 75 years. This information is retained pursuant to CBP records management schedule on Digital Forensics program. Information that does not lead to an individual's arrest, detention, or removal may be stored for 20 years after the matter is closed, consistent with the DHS records retention schedule N1-563-08-4-2.

### Information Sharing

There is no change to how the information is shared internal or external of DHS as a result of this update.

---

[12] *See supra* note 6.
[13] *See supra* note 2.

**Redress**

There are no changes to redress as a result of this update.

**Auditing and Accountability**

There are no changes to auditing and accountability as it relates to the new tools.

## Responsible Officials

Carl McClafferty
Associate Chief
U.S. Border Patrol Headquarters
Law Enforcement Operations Directorate
Intelligence Division
U.S. Customs and Border Protection
(202) 344-3388

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

## Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717