Privacy Impact Assessment
for the

U.S. Border Patrol

Digital Forensics Programs

DHS/CBP/PIA-053

April 6, 2018

Contact Point
Carla Provost
Acting Chief
United States Border Patrol
(202) 344-3159

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The 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 or administers, including laws relating to the detection and apprehension of illicit goods and individuals entering and exiting the United States. Depending on the circumstances, CBP searches of electronic devices are conducted pursuant to different legal authorities. CBP is conducting this Privacy Impact Assessment (PIA) to analyze standalone information technology systems designed to retain and analyze information collected from electronic devices collected pursuant to a warrant, abandonment, or when the owner consented to a search of the device, and to identify trends and patterns of illicit activities. ***This PIA does not include searches conducted pursuant to border search authority.*** CBP is publishing this PIA because the USBP digital forensic program collects, retains, and analyzes personally identifiable information (PII) obtained from electronic devices.

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 is charged with enforcing compliance with numerous federal laws at the border to prevent contraband, other illegal goods, and inadmissible persons from entering and exiting the United States. CBP enforces these laws both at and between Ports of Entry (POE).

CBP works to identify, interdict, and apprehend individuals with ties to terrorism, as well as individuals facilitating operations involving: human, drug, weapon, bulk cash, and other contraband smuggling activities. Consistent with this mission, CBP Officers and Agents collect information from a variety of sources to conduct interdiction operations and support criminal investigations. As part of CBP's border security duties, CBP may search and extract information from electronic devices, including but not limited to: laptop computers; thumb drives; compact disks; digital versatile disks (DVDs); mobile phones; subscriber identity module (SIM) cards; digital cameras; and other devices capable of storing electronic information.[1]

CBP Officers and Agents may search electronic devices in a variety of scenarios, including:

- **Border Search**. ***This PIA does not include searches conducted pursuant to border search authority.*** All travelers and the items they carry, including electronic devices, are subject to search by CBP when crossing the U.S. border. These searches apply to

[1] Unlike under CBP's border search authority, 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.

individuals seeking entry into or exit from the United States at the border or its functional equivalent, including at land, air, or sea POEs or at a location between POEs. CBP is authorized to conduct these searches to enforce immigration, customs, and other federal laws at the border. CBP provides notice and a thorough discussion of border searches of electronic devices in a newly updated PIA published in January 2018.[2] ***This PIA does not include searches conducted pursuant to border search authority.***

- **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**. Consent provided by the owner/possessor of the device may also authorize CBP to search the individual's electronic device. These searches usually are based on the belief that the device may contain information relevant to a law enforced or administered by CBP. The individual's consent may provide CBP authority to conduct the search in the absence of a warrant or other applicable authority. In this scenario, 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 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 the border zone). CBP may retrieve and search abandoned devices without any level of suspicion required.

When CBP encounters an electronic device pursuant to one of the scenarios listed above, the Officer or Agent may submit the electronic device for digital forensic analysis in accordance with

[2] *See* DHS/CBP/PIA-008(a) Border Searches of Electronic Devices (January 4, 2018), *available at* https://www.dhs.gov/privacy.
[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* https://www.cbp.gov/about/language-access.
[4] Generally, abandoned property in this context refers to personal property that a CBP Officer of Agent finds in the field or at the scene of a law enforcement action, and the individuals present disavow ownership of the property.

applicable law and policy. For the U.S. Border Patrol, typically, the Sector Intelligence Units at each U.S. Border Patrol Sector will have a dedicated team of trained Agents who conduct the forensic analysis of electronic devices obtained pursuant to a warrant, consent, or abandonment. If the Sector does not have appropriately trained Agents available, the Sector will store the electronic device consistent with CBP evidence handling procedures (described below) and request that the CBP Laboratories & Scientific Services Directorate (LSSD) provide technical assistance and analysis.[5] LSSD personnel regularly assist CBP Officers and Agents in crime scene processing, latent print examination, digital forensics, and controlled substance analysis; and serve as courtroom experts in the event of a prosecution to testify to chain of custody and other procedures.

General Examination Procedures

1. Security and Handling of Digital Evidence

All evidence obtained by U.S. Border Patrol requiring digital forensic processing is received, handled, and secured by the local Sector-based Evidence Collection Team (ECT) or a trained agent of a Sector Intelligence Unit, in accordance with CBP Seized Asset Management and Enforcement Procedures Handbook (SAMEPH), while maintaining a proper chain of custody at all times. Occasionally, there may be a need to conduct other forensic processes on digital media (DNA, latent prints, etc.). These situations are case-dependent, and the need for these other processes are coordinated with the requesting Border Patrol Agent prior to digital examination. The digital forensic examiner contacts appropriate ECT personnel for guidance on processing in order to avoid the destruction of forensic evidence.

2. Procedures for Requesting Examination

To request that digital forensic examiners conduct an examination, Agent/Officers must submit a signed request form accompanied by a signed Warrant, Consent Form (Appendix A), or Report of Investigation or Disposition Order by the Agent/Officer certifying in writing that the device was abandoned.

3. Documentation and Retention

Following the completion of the digital media examination, the data obtained from the

[5] Laboratories and Scientific Services Directorate (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 (WMD)-detection events, and coordinates expertise in interdiction and applied enforcement technologies.

device will be archived to appropriate media, including:

- Any photographs of the media and devices examined.
- Any exemplar or known files related to the case.
- Copies of any specialized software that may be needed to recreate the examination.
- Any tool specific logs, case files (*e.g.*, database indexes) or other files produced in the course of the examination.

Storage within an Information Technology System

If a Border Patrol Agent determines it is appropriate to conduct a forensic examination of an electronic device obtained pursuant to a warrant, consent, or abandonment, he or she may use an extraction tool to image the device and create a mirror copy of the data. Once the device is imaged, CBP uses tools to index and extract files and information, which can then be searched and analyzed. The extraction can be physical or logical. A physical extraction identifies and recovers data across the entire physical drive of a device, without regard to the file system in which the data may appear. A logical extraction identifies and recovers files and data from the operating system of the hardware, file systems, and applications residing on the hardware.

Following a search, if the electronic device yields information that is relevant to CBP's law enforcement missions, the Border Patrol Agent may load all information extracted from electronic device (unless it is excluded from the scope of a search warrant) into a standalone information technology (IT) system for analysis. The IT system used to store extracted digital information *may not* be connected to a CBP or DHS network.[6] For example, USBP acquired the "ADACS4" IT system to analyze data from electronic devices in order to discover connections, patterns, and trends related to terrorism, human and narcotic smuggling, and other activities posing a threat to border security.

Storing extracted information from an electronic device in an IT system permits queries of the stored data and makes associations based on both predetermined and ad hoc queries. These tools enable CBP to conduct a variety of analyses on electronic device data, to include: 1) timeframe analysis, which can help in determining when data was entered, modified, or deleted

[6] All employees who may view or access information extracted from a digital device sign a consent form acknowledging that by reviewing the contents of this report they may come into contact with potentially offensive material including, but not limited to, pornographic images, pornographic writings, offensive language, off-color language, or may in some other way be offensive. All digital media extractions are stored and examined on a secure, stand-alone computer because DHS has a strict policy against maintaining, circulating, or displaying any form of pornographic or offensive material on its computer networks, and deals with offenders in a strict manner. In addition, the extractions of electronic devices may contain viruses or malware, as well as programs not approved for use on the CBP network. By using a standalone system, USBP safeguards the CBP network, thus preventing the contamination or spread of any viruses and malware. The contents in the digital forensic examinations and report(s) should be reviewed in a limited access location, and on a computer not connected to the CBP network.

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.

CBP conducts searches to identify contraband or evidence relevant to the laws enforced or administered by CBP. If other violations of law, not under the purview of CBP, are encountered during the search, CBP may contact the appropriate DHS or external partner for appropriate action. CBP personnel trained to extract data from electronic media work with the Agent to determine what information is pertinent. The Agent then reviews all the information to assess whether there is relevant information that is within the scope of U.S. Border Patrol 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.

At the time of publication, ADACS4 is currently a stand-alone system in use solely by the United States Border Patrol. If the uses of ADACS4 expand, or if CBP develops an enterprise-wide solution for storing and searching, CBP will publish an update to this PIA.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

This PIA does not include searches conducted pursuant to border search authority.

CBP maintains information extracted from an electronic device in accordance with the following authorities:

- Title 6 of U.S. Code (U.S.C.): Domestic Security, including the following sections:
    - 6 U.S.C. § 111;
    - 6 U.S.C. § 112;
    - 6 U.S.C. § 203(1);
    - 6 U.S.C. § 211;
    - 6 U.S.C. § 251;
- Title 8 of U.S. Code: Aliens and Nationalities, and implementing regulations, including the following sections:
    - 8 U.S.C. § 1225(d), Authority relating to inspections;
    - 8 U.S.C. § 1357, Powers of immigration officers and employees;

- 8 C.F.R. § 287.2;
- 8 C.F.R. § 287.5;

- Title 19 of U.S. Code: Customs Duties, and implementing regulations, including the following sections:
  - 19 U.S.C. § 482, Search of vehicles and persons;
  - 19 U.S.C. § 507, Assistance for customs officers;
  - 19 U.S.C. § 1461, Inspection of merchandise and baggage;
  - 19 U.S.C. § 1462, Forfeiture;
  - 19 U.S.C. § 1496, Examination of baggage;
  - 19 U.S.C. § 1582, Search of persons and baggage; regulations;
  - 19 U.S.C. § 1589a, Enforcement authority of customs officers;
  - 19 U.S.C. § 1595a, Aiding unlawful importation; and
  - 19 C.F.R. § 161.2.

This PIA does not include searches conducted pursuant to border search authority. In addition to searches conducted under border search authority, CBP may conduct searches of electronic media under the following authorities: warrant search[7] (authorized by a judge/magistrate); consent search[8] (consent provided by the individual owning/possessing the device); and abandonment search[9] (unclaimed property that may or may not be associated with a criminal act). All of these searches are based on significant historical and legal precedent.

CBP and USBP have also issued several internal guidance documents to ensure compliance with law and policy regarding digital forensic examination of devices, including but not limited to:

- Chief, U.S. Border Patrol Memorandum, *Guidance on Searches of Cell Phones and Other Electronic Devices*, (1/21/2015);
- Chief, Tucson Sector Memorandum, *Procedural Guidance for Handling Subpoenas* (08/03/2011); and
- Chief, Tucson Sector Memorandum, *Administrative Subpoenas Procedural Guidance* (02/15/2012).

[7] Groh v. Ramirez, 540 U.S. 551, 558-59 (2004).
[8] United States. v. Andrus, 483 F.3d 711, 716-17 (10th Cir. 2007).
[9] United States v. Hernandez, 7 F.3d 944, 947 (10th Cir. 1993).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information that CBP collects, uses, and retains from electronic device searches may be retrieved by identifier, and thereby constitutes a Privacy Act system of records. CBP maintains electronic device information under the Border Patrol Enforcement Records (BPER) System of Records,[10] which applies to all records relating to securing the U.S. border between Ports of Entry, and the CBP Intelligence Records System (CIRS),[11] which applies to records collected to enhance CBP's ability to identify, apprehend, or prosecute individuals who pose a potential law enforcement or security risk; aid in the enforcement of the customs and immigration laws, and other laws enforced by DHS at the border; and enhance U.S. border security.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

USBP has worked with the CBP Office of Information Technology (OIT) and the CBP Laboratories and Scientific Services Directorate (LSSD) to meet the system security requirements for any information technology system that stores information extracted from an electronic device, including ADACS4. All information technology systems that store information extracted from an electronic device must receive an Authority to Operate from CBP OIT and be included in the CBP system inventory and subject to ongoing security assessments and controls, consistent with the requirements for all DHS networks and systems.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

USBP will retain records of arrest, detentions, removals, and associated information (such as information obtained from electronic devices) for up to 75 years. 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.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Extraction of information from electronic devices as described in this PIA is not subject to PRA requirements. Consent forms used by the various Sectors are also exempt from the PRA

[10] DHS/CBP-023 Border Patrol Enforcement Records System of Records, 81 FR 72601 (October 20, 2016).
[11] DHS/CBP-024 CBP Intelligence Records System System of Records, 82 FR 44198 (September 21, 2017).

which specifies "affidavits, receipts, changes of address, or consent" are not considered "information" under the PRA. Further, the PRA does not apply to information collections during "Federal criminal investigation or prosecution, or during the conduct of intelligence activities."[12]

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

CBP digital forensic examiners conduct examinations and analyses of, but not limited to: computer-related evidence such as personal data assistants, computers, storage devices, hard discs, memory cards, digital cameras, cellular phones, and digital video recordings. Digital information extracted from electronic devices may relate to both the owner of the device as well as his or her contacts and could include:

- Names;
- Phone numbers (pertaining to both the device owner and his or her contacts);
- Email addresses (stored within the contact folders on the mobile device);
- Text messages;
- Email messages;
- Call logs;
- Internet browsing history;
- Location information;
- Third-party apps and information stored therein;[13]
- Photo and video files;
- Any personal information that might be stored on the mobile device, such as credit card information, addresses, passwords, etc.; and
- Metadata associated with all of the categories listed above.

CBP uses digital information extracted from electronic devices for intelligence and for the enforcement and administration of laws within CBP's purview. If the extracted information is stored in an IT system, USBP may create customized searches to support a law enforcement action.

[12] Reference 5 C.F.R. 1320.3(h) and 44 U.S.C. § 3518(c).
[13] Unlike under CBP's border search authority, 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.

This PIA does not include searches conducted pursuant to border search authority.

For example, USBP uses the ADACS4 system to tailor searches to include only photo or video files, search the contents of the device based on a particular keyword, and generate reports that aggregate the data uploaded from the forensic extraction.

In support of the digital forensics request process, Sectors may develop a submission form for digital forensic support. Request forms may include the make, model, and provider of the device, and any associated case numbers from a relevant case management system such as E3/ENFORCE.[14] There is no interconnection with any DHS systems, however.

2.2 What are the sources of the information and how is the information collected for the project?

CBP digital information extracted from electronic devices obtained via warrant, consent, or abandonment includes information from individuals who are the subjects of investigations or prosecutions, witnesses, informants, and members of the public. The data itself may contain information on a variety of individuals, including those listed above as well as victims of crimes.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Digital information extracted from electronic devices may include information from publicly available sources (including social media). Concurrent to the digital extraction and analysis, CBP may search publicly available information based on the extracted data in order to verify or supplement information obtained from an electronic device.

2.4 Discuss how accuracy of the data is ensured.

CBP takes steps to ensure that digital information extracted from an electronic device is an exact copy of the original.[15] CBP creates a copy of the original electronic device (or the fields included in the logical extraction if the entire device is not examined) so that the original copy of the data is available for comparison. The mirror copy becomes the working copy in the standalone IT system, and is maintained as evidence for further use if necessary. For example, if the working copy becomes corrupt, forensic technicians can create a new clone by re-imaging the original electronic device. CBP uses hashing to guarantee the authenticity of an original data set. A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics

[14] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT *available at* https://www.dhs.gov/privacy.
[15] Logical extractions only acquire data from certain fields while the physical extraction collects data from the entire memory of the device. When a physical extraction is supported, CBP creates a mirror copy, which becomes the "working copy." This is common practice in order to maintain the integrity of the extraction. A physical extraction is not always possible on all devices.

of the data set; copied data that has been altered changes the hash value, enabling forensic technicians to identify the problem and distinguish the copy from the initial image.

Consistent with standard law enforcement practices, CBP will only take action against an individual based on information obtained from an electronic device if the information is assessed to be accurate and reliable. Typically, the information U.S Border Patrol obtains from an electronic device is used to corroborate existing evidence, rather than acting as primary indication of the commission of a crime. However, sometimes the evidence itself is indicative of a violation of law, such as child pornography.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Because of the volume and breadth of information maintained on and accessible by electronic devices, there is a risk of over-collection in that CBP may search and retain information that is not directly relevant to a law enforced or administered by CBP.

Mitigation: This risk is partially mitigated. CBP conducts focused searches using predetermined queries focused only on data relevant to the laws enforced or administered by CBP. After the extraction, the forensic technician will work with the requesting case agent to determine what information is relevant, and may deselect information deemed out of scope. Although these steps may reduce collection somewhat, some risk of over-collection remains since some datasets must be extracted in total to preserve their integrity. Further, because a complete mirror copy of the extraction may be required for forensic analysis, traditional mitigation measures such as manual deletion are not practical.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

USBP examines information from electronic devices 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 indicative of criminal activity. When the digital information extracted from an electronic device is stored in an IT system, USBP can conduct queries of all stored data and make associations based on both predetermined and ad hoc queries.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Using sector-specific standalone IT systems, USBP sifts through large amounts of information in response to user inquiry (such as a search based on a phone number) or programmed functions (an ongoing function that would create an alert when that phone number is encountered again) in order to produce results that may be useful in connection with a law enforcement activity. If USBP determines that any of the analytical results are useful to develop leads, identify trends associated with illicit activity, and further law enforcement actions, USBP will include the information in an enforcement case file or law enforcement intelligence product (*i.e.*, a field intelligence report) for dissemination. This information may also be used for prosecution of any violations.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. Each IT system that stores digital information extracted from an electronic device is a standalone system, only accessible by local users. However, if CBP develops an enterprise-wide IT solution to consolidate digitally information extracted from electronic devices, CBP will publish an update to this PIA.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that CBP will use forensic analysis of information from electronic devices to identify and target individuals based on religion, political views, and other activities protected by the First Amendment, or outside the scope of CBP's mission.

Mitigation: This risk is mitigated. Due to the variety and volume of information that may be housed in electronic devices, CBP may collect information related to activities protected by the First Amendment. However, CBP's collection of this information is incidental, and CBP's uses of data from electronic devices is limited to data relevant to the laws enforced and administered by CBP. DHS and CBP policies restrict the use of law enforcement activities that could potentially violate the law by targeting an individual's First Amendment rights. All CBP agents and officers are held to strict standards to uphold the law, and develop queries solely on the basis of performing CBP's law enforcement and border security functions, and not to make a determination based on an individual's religious or political views.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

As much as possible, CBP provides notice to the individual that holds the electronic device in question at the time of search and seizure for incidents occurring between POEs. A search warrant may also be the source of notice to an individual regarding the search of his or her electronic devices. CBP may opt not to provide notice in the event that alerting the individual of that fact may compromise an investigation or raise national security or officer safety concerns. In cases where CBP requests the owner's consent to search the device, CBP provides notice via a signed consent form that notifies the individual of his or her right to refuse or revoke consent to search. If the owner indicates he or she would like his or her device returned, a note is made on the consent form and the device is returned after the search is completed.[16]

CBP provides notice to the public that information collected from electronic devices may be incorporated into CBP systems of records. Information from devices searched and seized by CBP between official POEs is covered under the Border Patrol Enforcement Records SORN[17] and the CBP Intelligence Records System (CIRS) SORN.[18] This PIA also provides notice to the public of CBP's search, retention, and analysis of electronic devices.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

In some circumstances, CBP seeks consent for the search of an electronic device. In such cases, the individual may opt out and decline to provide the information, or withdraw consent at any time, at which point CBP may not continue the search based on a consensual basis. Nonetheless, USBP's searches of electronic devices in this context are pursuant to a warrant, consent, or abandonment. With a warrant, individual consent is not required, and there is no option to opt out. In the case of an abandoned device, CBP may not be able to identify the owner of the device, making consent to the search impractical.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that CBP has not provided sufficient notice to the public that

[16] All efforts are made to return devices to the owners. If the owner is in custody, devices are returned to the Seized Property Specialist who retains it with any other held property until the individual's case is adjudicated. If the owner is released on his or her own recognizance, he or she is notified in writing how and when the device/property can be retrieved. Any property unclaimed after 30 days is destroyed.
[17] DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[18] DHS/CBP-024 CBP Intelligence Records System System of Records, 82 FR 44198 (September 21, 2017).

digital information may be examined and copied from a searched, detained, or seized electronic device.

Mitigation: This risk is partially mitigated. In general, CBP provides notice to individuals for searches of electronic devices conducted pursuant to abandonment, warrant, or consent, as described in Section 4.1. In addition, CBP is publishing this PIA which, along with the SORNs listed above, provide notice of collection, use, and retention of information obtained from electronic devices. This PIA also provides notice that CBP may collect information from abandoned devices; however, there remains a risk that individuals will not have timely notice of CBP's retention of their data.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

USBP retains records of arrest, detentions, removals, and associated information (such as information obtained from electronic devices) for 75 years. 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.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that CBP will retain personal information obtained from abandoned electronic devices longer than necessary when it is not linked to any violation of a law enforced or administered by CBP.

Mitigation: This risk is mitigated. Information obtained from an abandoned device that does not lead to an individual's arrest, detention, or removal may be stored for 20 years after the matter is closed. Abandonment generally entails that the individual no longer "owns" the device, as they have manifested an intent to relinquish a possessory interest and the government then takes possession. A 20-year retention period is still necessary because determining whether an abandoned device is linked to unlawful activity cannot be fully assessed at the time of collection. In addition, information that is not immediately known to be of value may become valuable at a later point in time. Moreover, because information from abandoned devices is not flagged in any way and is co-located with other device data, there is no reliable way to differentiate and apply different retention rules.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Due to the law enforcement sensitive nature of the evidence retrieved from the devices as well as the possibility of explicit or offensive content, which may include pornographic images, pornographic writings, offensive language, violence, and other offensive material, dissemination of the evidence is strictly controlled and limited to those with a need-to-know.

Because CBP often collects information from electronic devices in connection with a law enforcement activity, it frequently shares this information in accordance with applicable law and policy with other federal agencies or state and local law enforcement agencies with a need-to-know, such as for joint law enforcement actions or in support of investigations. Less frequently, CBP may share the information with foreign law enforcement partners when a violation of the law may be global in scope.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The BPER and CIRS SORNs authorize sharing outside of DHS under the following conditions: to appropriate agencies and government organizations for investigating or prosecuting a violation of law (routine use G in both BPER and CIRS); for counterterrorism and intelligence purposes (routine use I in BPER and routine use Q in CIRS); to a court, magistrate, or administrative tribunal over the course of presenting evidence (routine use L in BPER); and to third parties during the course of a law enforcement investigation (routine use M in BPER and O in CIRS). CBP's sharing of information for investigations, prosecutions, and counterterrorism and intelligence is consistent with the original collection of records in support of CBP's border enforcement activities.

6.3 Does the project place limitations on re-dissemination?

Yes. Pursuant to the Third Agency Rule, CBP discloses information to third parties on the condition that any onward disclosure is first referred to CBP for approval. When the partner agency has prior knowledge of the need to share with a third party is required, CBP may authorize this sharing during the preliminary approval process.

Within CBP, when all processing of evidence is completed, the digital forensic examiner will notify the submitter and his or her supervisor. The examiner will create a CD/DVD/Blu-ray disc of the reports and affix an explicit content warning label to all CD/DVD evidence. Per the Sector Intelligence Unit Patrol Agent in Charge, the CD/DVD/Blu-ray and the target electronic

device will be released to the submitter's Supervisor or his or her designee. The agent/Supervisor retrieving the target electronic device and CD/DVD/Blu-ray will sign a form acknowledging receipt of these items, as well as the explicit content warnings contained on the Disclaimer Form and the chain of custody. Any additional party requesting a copy of the examination results must route that request through the original requesting party.

External to CBP, when all processing of evidence is completed, the digital forensic examiner will notify the submitter and will create a CD/DVD/Blu-ray of the reports to be returned along with the electronic device(s). The examiner will affix an explicit content warning label to all CD/DVD/Blu-ray evidence. The agent/representative retrieving the target electronic device and CD/DVD/Blu-ray will sign a form acknowledging receipt of the items, as well as the explicit content warnings contained in the Disclaimer Form and the chain of custody. Any additional party requesting a copy of the examination results must route that request through the original requesting party.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures that are made outside of CBP are typically made as a result of an ongoing investigation or other law enforcement activity, and the record of the disclosure is made in the pertinent case file. CBP uses the DHS Form 191 to record when it discloses information to a third party pursuant to the process described in Section 6.3 above.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information shared by CBP with partners for legitimate law enforcement purposes may be further disseminated by those partners for a different purpose.

Mitigation: This risk is mitigated because CBP notifies record recipients that it must not share the information with third parties without prior CBP approval. In the event that the partner is coordinating with another party for an investigation or prosecution, it will notify CBP at the outset, and CBP can approve this limited sharing in advance to ensure timely coordination between partners.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Specific to digital information extracted from an electronic device used in a law enforcement proceeding, a defendant or defendant's counsel have certain rights to examine any evidence as part of the pre-trial and trial process. In accordance with the Government's discovery

obligations and constitutional protections, the defense may be entitled to examine the electronic device or copies of information obtained therefrom.

Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law. In general, individuals seeking notification of and access to any record contained in CBP systems of records, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue, NW Room 3.3D
Washington, D.C. 20229

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "contacts."

Because of the law enforcement nature of CBP's collection of information from electronic devices, DHS has exempted portions of the applicable systems of records from the notification, access, amendment, and certain accounting provisions of the Privacy Act. Notwithstanding applicable exemptions, CBP reviews all such requests on a case-by-case basis. If compliance with a request would not interfere with or adversely affect the national security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of CBP in accordance with procedures and points of contact published in the applicable SORN.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If an individual believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
U.S. Customs and Border Protection
1300 Pennsylvania Avenue NW
Washington, D.C. 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries may be asked to provide additional identifying information to enable DHS to identify the record(s) at issue.

7.3 How does the project notify individuals about the procedures for correcting their information?

CBP provides general notice on its public-facing website about the procedures for submitting FOIA and Privacy Act requests and via the Federal Register. In addition, this PIA and the applicable SORNs provide further information about access and redress procedures.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that an individual may not have adequate redress in the event that information collected by CBP from another individual's electronic device is inaccurate and results in an adverse action of some kind.

Mitigation: This risk is partially mitigated. Electronic devices retain a wide range of data, which may include information linked to individuals not subject to an inquiry. Those individuals would likely not be aware that their information is housed within forensic analysis tools. In the event that erroneous information results in an individual encounter with CBP, he or she will have access to the redress procedures listed above. Absent such an encounter, the individual is unlikely to be aware of this information; as a result, some privacy risks remain unmitigated.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records.

Mitigation: This risk is partially mitigated. This PIA and the relevant SORNs describe how individuals can make access requests under FOIA or the Privacy Act. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access or correction of records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law

enforcement activities and may impose an impossible administrative burden on investigative agencies.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CBP maintains audit logs to identify misuse of the standalone IT system (*e.g.*, ADACS4), and any violation is handled through the disciplinary process, which includes referral to the Office of Professional Responsibility in appropriate cases. USBP is developing standard operating procedures that will establish standards for safeguarding and managing the information any information technology system that stores digital information extracted from an electronic device.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Digital forensic personnel undergo rigorous specialized, advanced training programs and hold numerous certifications related to this field of study. Personnel provide testimony as expert witnesses based on technical and other specialized knowledge, and the application of reliable principles and methods of digital evidence handling. Moreover, all CBP personnel are required to take annual privacy and information security training. Additionally, personnel authorized to use electronic media forensic technology are trained on the various tools and media data analysis systems before they are provided access to use them.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only authorized and trained CBP agents, officers, and analysts are permitted to use these specialized standalone IT systems. U.S. Border Patrol personnel must demonstrate a need-to-know (based on assignment as determined by the Patrol Agent in Charge of the Sector Intelligence Unit) in order to access the IT system and the information retained therein, and must sign the Forensic Report Disclaimer Form in which personnel acknowledge they may come into contact with offensive content. CBP has established privacy and information security training requirements and protocols for contractors and service providers, and tracks completion of annual privacy and information security training.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any new agreements to share the results of analysis derived from digital information extracted from an electronic device must be approved by the CBP Office of Chief Counsel, with review by the CBP Privacy and Diversity Office.

Responsible Officials

Carl McClafferty
Associate Chief
U.S. Border Patrol Headquarters
Law Enforcement Operations Directorate
Intelligence Division
U.S. Customs and Border Protection

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

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A: Example of a USBP Consent Form

U.S. Customs and Border Protection

Office of Border Patrol

CONSENT TO SEARCH AND/OR OPERATE CELLULAR TELEPHONE, OTHER ELECTRONIC DEVICE, OR SOCIAL MEDIA ACCOUNT

I acknowledge my constitutional right to refuse a search of my cellular phone, other electronic device and/or social media account hereinafter specified without a search warrant.

I acknowledge my right to refuse to consent to the memory of my cellular phone, other electronic device and/or social media account being searched without a search warrant.

I consent to a search of my cellular phone, other electronic device, and/or social media account. I understand that I can revoke this consent at any time.

This consent to search my electronic device extends to any and all applications or programs accessible on the device or a remote server. This includes law enforcement retrieving any information stored on the memory of the device, in a "cloud," on a website, or any other location where information may be stored.

I understand that anything discovered during such a search may be used against me in court including any criminal, civil, or administrative proceeding.

I hereby authorize Border Patrol to conduct a complete search of my cellular telephone or other electronic device, a _____ , serial number _____, password _____or social media account with the following identifying information _____and password _____, and to take therefrom any data files, or other information which they may desire, as well as operate (including, but not limited to, answering incoming calls, and text messages, and making calls or sending text messages from my device), post to, reply from, or otherwise manipulate my device or account.

I have given this authorization voluntarily and without threats, promises, pressure, or coercion of any kind.

Signature: _____

Date and Hour: _____ Place: _____

CERTIFICATION

I hereby certify that the foregoing was read to the above signatory, that he/she also read it, and has affixed his/her signature hereto.

_____
Border Patrol Agent Signature

_____ _____
Witness Signature Address

_____ _____
Interpreter Signature Language

_____
Interpreter Address

(TCA Revised 10/23/14)

This PIA does not include searches conducted pursuant to border search authority.