~~LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL

CBP's Searches of Electronic Devices at Ports of Entry - Redacted

~~LAW ENFORCEMENT SENSITIVE WARNING: The information in this document marked LES is the property of the Department of Homeland Security and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior Department of Homeland Security authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked LES on a website or unclassified network.~~

~~LAW ENFORCEMENT SENSITIVE~~

Homeland Security

December 3, 2018

OIG-19-10

DHS OIG Highlights

CBP's Searches of Electronic Devices At Ports of Entry

December 3, 2018

Why We Did This Audit

The *Trade Facilitation and Trade Enforcement Act of 2015* (TFTEA) requires U.S. Customs and Border Protection (CBP) to establish standard operating procedures (SOP) for searching, reviewing, retaining, and sharing information in communication, electronic, or digital devices at U.S. ports of entry. The TFTEA also requires the DHS Office of Inspector General to conduct three annual audits to determine to what extent CBP conducted searches of electronic devices in accordance with the SOPs.

What We Recommend

We made five recommendations to improve CBP's oversight of searches of electronic devices at ports of entry.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Between April 2016 and July 2017, CBP's Office of Field Operations (OFO) did not always conduct searches of electronic devices at U.S. ports of entry according to its SOPs. Specifically, because of inadequate supervision to ensure OFO officers properly documented searches, OFO cannot maintain accurate quantitative data or identify and address performance problems related to these searches. In addition, OFO officers did not consistently disconnect electronic devices, specifically cell phones, from the network before searching them because headquarters provided inconsistent guidance to the ports of entry on disabling data connections on electronic devices.

OFO also did not adequately manage technology to effectively support search operations and ensure the security of data. Finally, OFO has not yet developed performance measures to evaluate the effectiveness of a pilot program, begun in 2007, to conduct advanced searches, including copying electronic data from searched devices to law enforcement databases.

These deficiencies in supervision, guidance, and equipment management, combined with a lack of performance measures, limit OFO's ability to detect and deter illegal activities related to terrorism; national security; human, drug, and bulk cash smuggling; and child pornography.

CBP's Response

CBP concurred with our recommendations. We have included a copy of CBP's response to our draft report at appendix A.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

December 3, 2018

MEMORANDUM FOR: Todd Owen
Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

FROM: Sondra F. McCauley
Assistant Inspector General for Audits

SUBJECT: *CBP's Searches of Electronic Devices at Ports of Entry*

Attached for your action is our final report, *CBP's Searches of Electronic Devices at Ports of Entry*. We incorporated the formal comments provided by your office.

The report contains five recommendations aimed at improving the overall effectiveness of CBP's oversight of searches of electronic devices at ports of entry. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider the five recommendations resolved and open. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence showing completion of the agreed-upon corrective actions. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Donald Bumgardner, Deputy Assistant Inspector General for Audits, at (202) 981-6000.

Background

U.S. Customs and Border Protection (CBP) exercises law enforcement authority when securing the Nation's borders and 328 ports of entry. Electronic devices, such as computers, thumb drives, and mobile phones, are subject to search at U.S. ports of entry to ensure the enforcement of immigration, customs, and other Federal laws.

CBP processed more than 787 million travelers upon arrival at U.S. ports of entry in fiscal years 2016 and 2017, and searched approximately 47,400 electronic devices. In fiscal year 2016, CBP processed more than 390 million travelers arriving at U.S. ports of entry and searched the electronic devices of an estimated 18,400 of those inbound travelers (.005 percent). In FY 2017, CBP processed more than 397 million travelers and searched the electronic devices belonging to more than 29,000 of those inbound travelers (.007 percent).

CBP's Office of Field Operations (OFO) is responsible for determining the admissibility of travelers at U.S. ports of entry. OFO officers conduct primary inspections of all travelers arriving at ports of entry. During a primary inspection, OFO officers review travelers' passports and other documents to decide whether to admit travelers to the United States or refer them for secondary inspection.

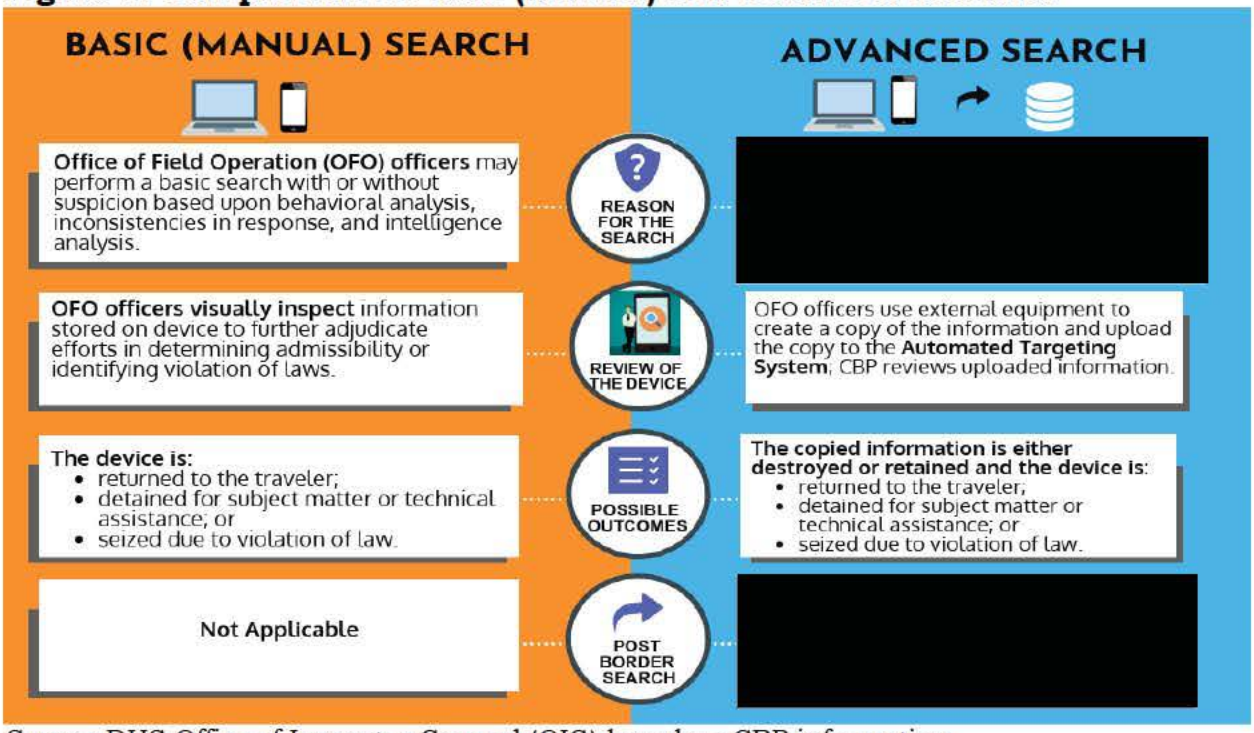
During secondary inspection, an OFO officer may search a traveler's electronic device to determine admissibility and identify any violation of laws. For instance, in March 2018, during a search of a traveler's electronic device, officers found images and videos of terrorist-related materials. In another incident, officers found graphic and violent videos, including child pornography. CBP denied both travelers entry into the United States.

A secondary inspection may involve a basic (manual) search, an advanced search, or both. The officer can make a referral for a manual search because of inconsistencies in response, behavioral analysis, or intelligence analysis. A manual search involves the OFO officer manually reviewing the information on a traveler's electronic device.

An advanced search, which OFO started as a pilot program in 2007, involves a specially trained officer connecting external equipment to the traveler's device to copy information. The officer uploads the copied information to CBP's Automated Targeting System (ATS) to be further analyzed against existing ATS information. CBP personnel provide real-time feedback to the OFO officer of any identified derogatory information.

After a secondary inspection, CBP personnel analyze the copied information in ATS and other information provided by partner agencies to link unlawful activities related to counterterrorism, narcotics, illicit trade, human smuggling, and special interest aliens.[1] ATS is updated, as appropriate, based on CBP's analysis. [redacted] See figure 1.

Figure 1. Comparison of Basic (Manual) and Advanced Searches



Source: DHS Office of Inspector General (OIG) based on CBP information

The *Trade Facilitation and Trade Enforcement Act of 2015*, Pub. L. No. 114-125 (TFTEA), enacted on February 24, 2016, requires CBP to establish standard operating procedures (SOP) for searching, reviewing, retaining, and sharing information contained in communication, electronic, or digital devices encountered at U.S. ports of entry. CBP must review and update these SOPs every 3 years.[2]

CBP has issued a series of memorandums and SOPs to govern searches of electronic devices at ports of entry. According to CBP's SOPs, all searches of electronic devices require supervisory notification. In addition, according to an

[1] Special interest aliens are aliens from special interest countries, which are generally defined as countries that are of concern to the national security of the United States, based on several U.S. Government reports.
[2] TFTEA, § 802(a) (codified as 6 United States Code (USC) 211(k)(1)(A)).

April 2015 memorandum, an OFO officer may only conduct an advanced search if the traveler [redacted]

[redacted]

CBP uses the TECS[3] module called Inspection Operations of Electronic Media, also known as an electronic media report (EMR), to document the border searches of electronic devices. The EMR provides information of the search, such as the device details, type of search performed on the device, and the officer's remarks of the inspection. In instances in which CBP detains or seizes an electronic device, CBP documents such incidents on CBP forms 6051D[4] and 6051S,[5] respectively, to demonstrate CBP's chain of custody.

The TFTEA also requires DHS OIG to conduct audits to determine whether CBP is searching electronic devices in conformity with its SOPs and to compile and report the following information:

- a description of the activities of CBP officers and agents with respect to such searches;
- the number of such searches;
- the number of instances in which information contained in such devices that were subjected to such searches was retained, copied, shared, or entered in an electronic database;
- the number of such devices detained as the result of such searches; and
- the number of instances in which information collected from such devices was subjected to such searches and transmitted to another Federal agency, including whether such transmissions resulted in a prosecution or conviction.[6]

In this report, we present the results of our audit to determine whether CBP conducted searches of electronic devices in accordance with SOPs. Appendix B contains other information we are required to report under the TFTEA.

[3] TECS is not an abbreviation. It is the official name of the system.
[4] *Detention Notice and Custody Receipt for Detained Property* (CBP Form 6051D).
[5] *Custody Receipt for Seized Property and Evidence* (CBP Form 6051S).
[6] TFTEA, § 802(a) (codified as 6 USC 211(k)(5)).

Results of Audit

During our review of a sample of border searches of electronic devices conducted between April 2016 and July 2017, we determined that OFO did not always conduct the searches at U.S. ports of entry according to its SOPs. Specifically, because of inadequate supervision to ensure OFO officers properly documented searches, OFO cannot maintain accurate quantitative data or identify and address performance problems related to these searches. In addition, OFO officers did not consistently disconnect electronic devices, specifically cell phones, from networks before searching them because headquarters provided inconsistent guidance to the ports of entry on disabling data connections on electronic devices. OFO also did not adequately manage technology to effectively support search operations and ensure the security of data. Finally, OFO has not yet developed performance measures to evaluate the effectiveness of a pilot program, begun in 2007, to conduct advanced searches, including copying electronic data from searched devices to law enforcement databases.

These deficiencies in supervision, guidance, and equipment management, combined with a lack of performance measures, limit OFO's ability to detect and deter illegal activities related to terrorism; national security; human, drug, and bulk cash smuggling; and child pornography.

Searches of Electronic Devices Not Always Properly Documented

OFO officers did not always properly document actions and complete the required chain of custody forms when conducting searches of electronic devices. This occurred because supervisors did not always adequately review documentation to ensure officers properly documented searches at the ports of entry.

CBP Directive 3340-049, *Border Search of Electronic Devices Containing Information*, dated August 20, 2009, was in effect at the time of our review. According to the directive, CBP officers are responsible for completing all applicable documentation in the appropriate CBP systems of record when conducting electronic searches. Reports are to be created and updated in an accurate, thorough, and timely manner. Reports must include all information related to the search through the final disposition, including supervisory approvals and extensions when appropriate. In addition, the duty supervisor is to ensure the officer completes a thorough inspection and that all notification, documentation, and reporting requirements are accomplished.

We reviewed 194 EMRs and identified 130 (67 percent) that featured one or more problems, which totaled 147 overall. See table 1.

Table 1: Problems Identified in CBP Electronic Media Reports

Insufficient or Inaccurate Information	**Number of EMRs**
Vague narrative describing border search	62
Inaccurate notes or action details	31
No witnessing supervisor documented	29
Detention and Seizure Chain of Custody Forms	
Missing information on Forms 6051D & 6051S	7
Late Supervisory Review	
Review more than 7 days from incident	18

Source: OIG analysis of EMRs from CBP

Without accurate and complete documentation of border searches of electronic devices, OFO cannot maintain reliable quantitative data, identify and address performance problems, and minimize the risk of electronic devices becoming lost or misplaced.

Data Connections Not Consistently Disabled Prior to Searching Electronic Devices

A border search of an electronic device conducted by an OFO officer should include an examination of only the information that is physically on the device, not information stored on a remote server. To avoid retrieving or accessing information stored remotely, officers should either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode) or, in instances warranted by national security, law enforcement, officer safety, or other operational considerations, officers will disable network connectivity. However, OFO officers did not consistently disconnect electronic devices, specifically cell phones, from the network before searching them. This occurred because headquarters provided inconsistent guidance to the ports of entry on disabling electronic devices' data connections.

Specifically, in April 2017, OFO issued a memo[7] that claimed to reaffirm its existing policy and protocol for disconnecting electronic devices from internet access (i.e., disabling network connections) before a search.[8] Unless each device's network connection is disabled, OFO could potentially retrieve information from external sources, leaving the results of the border search questionable. However, Directive 3340-049, the policy at the time, did not require disabling data connections prior to conducting a search. Of the 194 EMRs we reviewed, 154 were completed prior to the issuance of the April 2017

[7] *Border Search of Electronic Devices Containing Information*, dated April 13, 2017.
[8] Disabling data connections ensures that electronic devices are limited to the data on them.

memo. None of the 154 contained evidence that data connections were disabled on electronic devices searched.

In addition, the April 2017 memo required OFO officers to document in the EMR whether cellular and data connections were disabled prior to conducting a search and further required supervisors to confirm connections were disabled in a statement in the EMR before approving it. Despite these requirements, OFO supervisors did not provide adequate oversight to ensure officers disabled data connections on electronic devices prior to searching them, nor did the supervisors properly review EMRs. We reviewed 40 EMRs completed after the issuance of the April 2017 memo. Even though OFO supervisors reviewed and approved EMRs, more than one-third of the EMRs (14 of 40) lacked a statement confirming that the electronic device's data connection had been disabled.

Since we began the audit, CBP has taken action to improve in this area. In October 2017, CBP completed system enhancements to their EMRs in TECS. Those enhancements include a mandatory data field to allow officers to select, rather than compose, a statement to confirm disabling a device data connection. Additionally, on January 4, 2018, CBP issued Directive 3340-049A, *Border Search of Electronic Devices*, which supersedes Directive 3340-049. Unlike the superseded directive, the newly issued directive expressly states, "Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode); or, where warranted by national security, law enforcement, officer safety, or other operational considerations, officers will themselves disable network connectivity."

External Equipment and Data for Border Searches Not Well Managed

According to the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, Sections 10.03 and 12.01, management is responsible for establishing physical control to secure and safeguard vulnerable assets and implement control activities through policies. However, OFO is not managing the external equipment used to conduct advanced border searches of electronic devices well. Specifically, OFO did not renew software licensing agreements for external equipment expeditiously and maintained information copied on thumb drives that should have been deleted.

OFO Did Not Renew Software Licensing of External Equipment Expeditiously

OFO purchased the [redacted] tool, which is a computer triage tool that enables examination of laptop hard drives, USB[9] drives, and multimedia cards, to prohibit importation of illegal materials. The [redacted] tool requires an annual license renewal that encompasses a warranty, support, maintenance, and software upgrades to maximize security effectiveness. We reviewed software licensing agreements of the [redacted] tool from 2016 and 2017 and found a licensing lapse. Because OFO headquarters did not renew the software licensing of the [redacted] tool expeditiously, licensing agreements were only in effect from January 20, 2016, through January 31, 2017; and from September 13, 2017, through September 12, 2018.

Software licensing agreements were **not** in effect from February 1, 2017, through September 12, 2017.

According to an OFO official, there is no dedicated funding for external equipment such as the [redacted] tool because it is part of the advanced searches of electronic devices pilot program. According to the same official, due to the lack of dedicated funding and the combination of budgetary issues and other funding priorities, the initial vendor estimate he received for the purchase expired. Therefore, he had to obtain another vendor estimate, which caused a delay in promptly submitting the license renewal documentation.

Without a valid software license, OFO officers could not conduct advanced searches of laptop hard drives, USB drives, and multimedia cards at the ports of entry. This deficiency limited OFO's ability to obtain evidence of criminal activity and to detect and deter illegal activities, such as child pornography. Additionally, it hinders OFO's ability to mitigate the risk of criminals entering the United States with unexamined national security or law enforcement-related information on their laptops.

OFO Does Not Always Delete Travelers' Information Copied during Advanced Searches

During advanced searches, OFO officers connect external equipment to electronic devices and copy information onto a thumb drive; the copied information is uploaded via the thumb drive to the CBP's ATS for further analysis. According to two OFO training officials, once an OFO officer completes an ATS upload, he or she should immediately delete all copied information from the thumb drive, but OFO could not provide written policy or procedures related to the training officials' oral requirement.

[9] Universal Serial Bus is a common interface that enables communication between devices and a host controller such as a personal computer.

We physically inspected thumb drives at five ports of entry. At three of the five ports, we found thumb drives that contained information copied from past advanced searches, meaning the information had not been deleted after the searches were completed. Based on our physical inspection, as well as the lack of a written policy, it appears OFO has not universally implemented the requirement to delete copied information, increasing the risk of unauthorized disclosure of travelers' data should thumb drives be lost or stolen.

OFO Has Not Developed Performance Measures for the Advanced Searches of Electronic Devices Pilot Program

According to GAO's *Standards for Internal Control in the Federal Government*, management should establish activities to monitor performance measures and indicators. These may include comparisons and assessments relating different sets of data to one another so that analyses of the relationships can be made and appropriate actions taken.

OFO has not developed performance measures to assess the effectiveness of its advanced searches of electronic devices pilot program. In 2007, four ports of entry used external equipment for OFO's advanced searches of electronic devices pilot program; OFO has now expanded the pilot to 67 ports of entry. Although OFO maintains quantitative data on the number and location of advanced searches, it has not developed performance measures. One area to measure is the number of instances in which information collected from searches resulted in a prosecution or conviction, but according to OFO, it does not track this information.

Without performance measures, OFO cannot evaluate the effectiveness of the pilot program. OFO will not be able to determine whether the advanced searches are achieving their intended purpose or whether the use of advanced searches should be expanded to other ports of entry.

Conclusion

In FY 2017, CBP searched electronic devices belonging to more than 29,000 inbound travelers. Given the number of searches, it is important that OFO ensure the searches are properly documented and that OFO officers conducting the searches are adequately overseen. Properly managing the equipment used to conduct advanced searches is also critical to make certain officers are not limited in their ability to detect and deter illegal activities. As the world of information technology evolves, techniques used by OFO must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes. Finally, to demonstrate OFO is meeting its security mission, developing performance measures will be essential to assess the effectiveness of OFO's pilot program of advanced searches, which has been

in place for 10 years.

Recommendations

Recommendation 1: We recommend the Executive Assistant Commissioner for the Office of Field Operations ensure its officers properly document their actions when conducting searches of electronic devices, and supervisors provide adequate and prompt review of electronic media reports and related information.

Recommendation 2: We recommend the Executive Assistant Commissioner for the Office of Field Operations ensure supervisors oversee the disabling of data connections prior to conducting searches of electronic devices.

Recommendation 3: We recommend the Executive Assistant Commissioner for the Office of Field Operations ensure all equipment used during advanced searches is accounted for and all software licenses are renewed expeditiously.

Recommendation 4: We recommend the Executive Assistant Commissioner for the Office of Field Operations ensure that travelers' copied information is immediately deleted from thumb drives after successful upload to the Automated Targeting System.

Recommendation 5: We recommend the Executive Assistant Commissioner of the Office of Field Operations:

a) Develop and implement performance measures for the advanced searches of electronic devices pilot program.
b) Evaluate the effectiveness of the pilot program to determine whether the advanced searches are achieving the program's intended purpose.
c) Work with the Commissioner of U.S. Customs and Border Protection to evaluate the performance of Office of Field Operations in the advanced searches of electronic devices pilot program and, based on the results of such evaluation, decide whether to discontinue or establish it as a permanent program of record.

Management Comments and OIG Analysis

CBP concurred with the recommendations. Appendix A contains a copy of CBP's management comments in their entirety. We also received technical comments and incorporated them in the report where appropriate. We consider the five recommendations to be resolved and open. A summary of CBP's responses and our analysis follows.

CBP Response to Recommendation 1: CBP concurred with the recommendation. OFO Tactical Operations Division's (TOD) National Program Managers will provide oversight of EMRs on a monthly basis. TOD is developing a process to conduct annual Field Office reviews at the ports of entry. TOD will work with OFO's Planning, Program Analysis and Evaluation (PPAE) Directorate to enhance and update the current self-inspection worksheet to ensure the worksheet addresses proper documentation of officer actions when conducting searches of electronic devices. CBP estimates these actions will be completed by June 30, 2019.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive documentation showing that CBP has begun providing oversight of EMRs on a monthly basis and developed a process for annual reviews at the ports of entry, as well as incorporated use of the self-inspection worksheet.

CBP Response to Recommendation 2: CBP concurred with the recommendation. OFO is developing a process to conduct annual Field Office reviews that will observe operations and procedures in place to ensure that supervisors oversee the disabling of data connections prior to conducting a search of an electronic device. TOD will also work with OFO PPAE to enhance and update the current self-inspection worksheet to ensure the worksheet addresses proper documentation of officer actions when conducting searches of electronic devices, as well as adequate and prompt supervisory reviews. CBP estimates these actions will be completed by June 30, 2019.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive documentation showing that CBP has developed a process for annual Field Office reviews to oversee disabling data connections and incorporated the self-inspection worksheet.

CBP Response to Recommendation 3: CBP concurred with the recommendation. OFO is developing a process to conduct annual Field Office reviews at ports of entry. The TOD National Program Managers will observe operations and procedures in place to ensure that software licenses are

promptly renewed annually. CBP estimates these actions will be completed by June 30, 2019.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive documentation showing that CBP has developed a process to conduct annual Field Office reviews to ensure that software licenses are renewed annually.

CBP Response to Recommendation 4: CBP concurred with the recommendation. The TOD National Program Managers will observe operations and procedures that ensure supervisors oversee travelers' copied information is immediately deleted from the thumb drives after successful uploads to the ATS. OFO is developing a process to conduct annual Field Office reviews at ports of entry. TOD will work with OFO PPAE to enhance and update the current self-inspection worksheet. CBP estimates these actions will be completed by June 30, 2019.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive documentation showing that CBP has developed a process to conduct annual Field Office reviews to ensure that travelers' copied information is deleted from the thumb drives.

CBP Response to Recommendation 5: CBP concurred with the recommendation. CBP OFO will develop performance measures based on positive enforcement actions resulting from an advanced search. The performance measures will be evaluated by positive results achieved to determine if goals are being accomplished. CBP will evaluate the effectiveness of the pilot program to determine whether the advanced searches are achieving the program's intended purpose. CBP will finalize the transformation of the program to a national program of record. CBP estimates these actions will be completed by January 31, 2019.

OIG Analysis: We consider these actions responsive to the recommendation, which is resolved and open. We will close this recommendation when we receive documentation showing that CBP has developed performance measures, evaluated the effectiveness of the pilot program, and finalized the transformation of the program to a program of record.

Objective, Scope, and Methodology

The Department of Homeland Security, Office of Inspector General was established by the *Homeland Security Act of 2002*, Pub. L. No. 107-296, by amendment to the *Inspector General Act of 1978*.

This audit is the first of three annual audits required by the *Trade Facilitation and Trade Enforcement Act of 2015*, Pub. L. No. 114-125 (TFTEA). We conducted this audit to determine to what extent CBP conducted searches of electronic devices at U.S. ports of entry in accordance with its SOPs. For the purposes of this audit, our scope was limited to OFO's operations in conducting searches of electronic devices at ports of entry. To achieve our audit objective, we:

- interviewed CBP officials in OFO, Laboratories and Scientific Services Directorate, Office of Information & Technology, Office of Chief Counsel, United States Border Patrol, and Air & Marine Operations;
- reviewed the TFTEA; CBP Directive 3340-049, *Border Search of Electronic Devices Containing Information* (Issued August 20, 2009); CBP Directive 3340-049A, *Border Search of Electronic Devices* (Issued January 4, 2018); and memorandums and muster documents relating to border searches of electronic devices;
- reviewed privacy impact assessments, contract documents, and training documents;
- conducted five site visits from July 2017 to September 2017 to Dulles International Airport, Miami International Airport, Miami Seaport, El Paso Land Port, and Buffalo Land Port;
- attended training on advanced searches of electronic devices;
- interviewed OFO officers, border security coordinators, program managers, training officers, and OFO supervisors at the ports of entry we visited; and
- physically inspected equipment used to conduct advanced searches at the ports of entry visited.

Additionally, we judgmentally selected and reviewed a sample of 194 electronic media reports completed between April 2016 and July 2017 at Dulles International Airport, Miami International Airport, Miami Seaport, El Paso Land Port, Buffalo Land Port, and Los Angeles Airport.

We assessed the reliability of the data received from OFO pertaining to the number of search incidents. The data included the total number of electronic searches, basic (manual) searches, and advanced searches. We assessed the reliability of the data by (1) interviewing OFO officials knowledgeable about the data, and (2) comparing data that OFO provided to OIG to CBP's publicly released statistical data information. We identified discrepancies of less than 1 percent. We determined that the data were the best available at the time. Despite the discrepancies, the data were sufficient for the purposes of our audit. For the number of devices detained, we reported the data as provided by OFO. See appendix B.

We conducted this performance audit between December 2016 and May 2018 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

The Office of Audits major contributors to this report are Patrick O'Malley, Audit Director; Modupe Ogunduyile, Audit Manager; Jason Kim, Auditor-in-Charge; Rolando Chavez, Auditor; Enrique Leal, Auditor; Nedra Rucker, Auditor; Kelly Herberger, Kevin Dolloson and Ellen Gallagher, Communications Analysts; and Kathy Hughes, Independent Referencer.

Appendix A
CBP's Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

September 10, 2018

MEMORANDUM FOR: Sondra F. McCauley
Acting Assistant Inspector General for Audits
Office of the Inspector General

FROM: Henry A. Moak Jr. 9/10/18
Acting Chief Accountability Officer
U.S. Customs and Border Protection

SUBJECT: Management Response to Draft Report: "CBP's Searches of Electronic Devices at Ports of Entry"
(Project No. 17-007-AUD-CBP)

Thank you for the opportunity to review and comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

It is important to note that border searches of electronic devices are conducted in furtherance of CBP's customs, immigration, law enforcement, and homeland security responsibilities and to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce and administer. As the OIG's draft report acknowledges, CBP processed more the 787 million travelers upon arrival at ports of entry during fiscal years (FY) 2016 and 2017, and searched only approximately 47,400 electronic devices during that time, affecting only 0.007 percent of travelers. These searches identified evidence helpful in combating terrorist activity, child pornography, human trafficking, violations of export controls, intellectual property rights violations, and visa fraud. Electronic device searches are also integral in some cases to determining an individual's intentions upon entering the United States and provide additional information relevant to admissibility under the immigration laws.

CBP is committed to continuing to fulfill its responsibility for ensuring the safety and admissibility of the goods and people entering the United States and exercising its border search authority in accordance with its statutory and constitutional authority. CBP's authority to conduct search of inspections of persons and merchandise crossing out nation's border is longstanding and well-established. CBP continues to process more than 1 million travelers arriving to the United States each day. Searches of electronic

devices have remained consistent during FY 2017, averaging fewer than 2,500 arriving international travelers per month.

On January 5, 2018, CBP released an update to the agency's public Directive governing Border Search of Electronic Devices, CBP Directive No. 3340-049A. This Directive, which supersedes the previous directive released in August 2009, enhances transparency, accountability, and oversight of electronic device border searches performed by CBP.

The draft report contained five recommendations, all with which CBP concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: DHS Management Response to Recommendations Contained in (Project No. 17-007-AUD-CBP)

The Office of Inspector General (OIG) recommended that the U.S. Customs and Border Protection (CBP) Executive Assistant Commissioner, Office of Field Operations (OFO):

Recommendation 1: Ensure its officers properly document their actions when conducting searches of electronic devices, and supervisors provide adequate and prompt review of electronic media reports and related information.

Response: Concur. CBP's 2009 Directive on Border Search of Electronic Devices Containing Information, CBP Directive 3340-049 (the "2009 Directive") provided that searches of electronic devices should be conducted in the presence of a supervisor and, "[i]n circumstances where operational considerations prevent a supervisor from remaining present for the entire search, or where supervisory presence is not practicable, the examining Officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof." CBP's updated Directive on Border Search of Electronic Devices, CBP Directive 3340-049A, issued on January 4, 2018 (the "2018 Directive"), now requires supervisory approval at the Grade 14 level or higher (or a manager with comparable responsibilities), in order to perform an advanced search[1] of an electronic device.

To ensure that CBP policy is being followed, the CBP OFO Tactical Operations Division's (TOD) National Program Managers (NPM) will monitor, review, and conduct random reviews of Inspection Operations of Electronic Media (IOEM) on a monthly basis. OFO is also developing a process to conduct annual Field Office reviews at the Ports of Entry (POE) to ensure documentation of actions are input properly, to include supervisory review.

TOD will work with the OFO, Planning, Program Analysis and Evaluation Directorate, Quality Assurance Enterprise Division, to enhance and update the current self-inspection worksheet to ensure that the self-inspection worksheet addresses proper documentation of officer actions when conducting searches of electronic devices, as well as adequate and prompt supervisory reviews of reports and related information. Estimated Completion Date (ECD): June 30, 2019

Recommendation 2: Ensure supervisors oversee the disabling of data connections prior to conducting searches of electronic devices.

---

[1] The 2018 Directive defines "advanced search" as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents."

Response: Concur. CBP has already taken steps to improve processes designed to ensure that data connections are disabled prior to conducting searches of electronic devices. In an update to CBP's public-available policy on border searches of electronic devices, the 2018 Directive expressly states that, during the course of a border search of an electronic device, CBP Officers may not intentionally use the device to access information that is solely stored remotely. In order to avoid retrieving or accessing information stored remotely and not otherwise present on the device, the 2018 Directive further requires CBP Officers to "either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity."

OFO is also developing a process to conduct annual Field Office reviews. During the Field Office reviews, the TOD NPMs will observe operations and procedures in place (SOP/checklist) that ensure supervisors oversee the disabling of data connections prior to conducting a search of an electronic device. TOD will also work with the OFO, Planning, Program Analysis and Evaluation Directorate, Quality Assurance Enterprise Division, to enhance and update the current self-inspection worksheet to ensure that the self-inspection worksheet addresses proper documentation of officer actions when conducting searches of electronic devices, as well as adequate and prompt supervisory reviews of reports and related information. ECD: June 30, 2019

Recommendation 3: Ensure all equipment used during advanced searches is accounted for and all software licenses are renewed expeditiously.

Response: Concur. OFO is developing a process to conduct annual Field Office reviews at the Ports of Entry (POE) to ensure documentation of actions are input properly, to include supervisory review and equipment is accounted for, in working order and the license is not expired . During Field Office reviews, the TOD NPMs will observe operations and procedures in place (SOP/checklist) that ensure supervisors check equipment daily to validate that all equipment is accounted for, working properly and software licenses are renewed. The TOD NPMs will ensure that DOMEX equipment licenses are promptly renewed annually.

TOD will work with the OFO, Planning, Program Analysis and Evaluation Directorate, Quality Assurance Enterprise Division, to enhance and update the current self-inspection worksheet to ensure that the self-inspection worksheet addresses proper documentation of officer actions when conducting searches of electronic devices, as well as adequate and prompt supervisory reviews of reports and related information. ECD: June 30, 2019

Recommendation 4: During the field audit reviews, the TOD's NPMs will observe operations and procedures in place (SOP/checklist) that ensures supervisors oversee that

travelers' copied information is immediately deleted from the thumb drives after successful uploads to the Automated Targeting System.

Response: Concur. OFO is developing a process to conduct annual Field Office reviews at the Ports of Entry (POE) to ensure documentation of actions are input properly, to include supervisory review.

TOD will work with the OFO, Planning, Program Analysis and Evaluation Directorate, Quality Assurance Enterprise Division, to enhance and update the current self-inspection worksheet to ensure that the self-inspection worksheet addresses proper documentation of officer actions when conducting searches of electronic devices, as well as adequate and prompt supervisory reviews of reports and related information. ECD: June 30, 2019

Recommendation 5: (A) Develop and implement performance measures for the advanced searches of electronic devices pilot program. (B) Evaluate the effectiveness of the pilot program to determine whether the advanced searches are achieving the program's intended purpose. (C) Work with the Commissioner of U.S. Customs and Border Protection to evaluate the performance of Office of Field Operations in the advanced searches of electronic devices pilot program and, based on the results of such evaluation, decide whether to discontinue or establish it as a permanent program of record.

Response: Concur. CBP OFO will take the following actions: (A) Develop performance measures that will measure based on positive enforcement actions resulting from an advanced search. Examples of positive enforcement actions include the discovery of unlawful activity leading to counter-network investigations of terrorism, information related to national security, drug trafficking, human smuggling and/or human trafficking, child pornography, weapons trafficking, admissibility and immigration violations, currency smuggling and other transnational organized crimes. The performance measures will be evaluated by positive results achieved to determine if goals are being accomplished. (B) Evaluate the effectiveness of the pilot program to determine whether the advanced searches are achieving the program's intended purpose. The program will be evaluated using performance measures based on positive enforcement actions resulting from an advanced search. (C) Finalize the transformation of the program to a national program of record. ECD: January 31, 2019

5

Appendix B
OIG Information to be Reported under the Trade Facilitation and Trade Enforcement Act of 2015

As required under the TFTEA, in the background and results sections of this report, we described the activities of CBP officers and agents with respect to electronic searches.

Other reportable information in table 2 shows the total number of border searches of electronic devices in FY 2016 and FY 2017; the number of manual and advanced searches (conducted using external equipment); and the number of electronic devices detained as a result of electronic searches. However, as noted in table 2, we were not able to determine the number of instances in which information collected from electronic devices was subjected to these searches and was transmitted to another Federal agency or whether such transmissions resulted in a prosecution or conviction because OFO does not track this information.

Table 2: Border Searches of Electronic Devices, FYs 2016–2017

Number of Searches	**FY 2016**	**FY 2017**
Total Electronic Border Searches*	19,148	30,385
Basic (manual) search	16,725	27,701
Advanced search**	2,423	2,684
Information collected was transferred to another Federal agency, including whether such transmissions resulted in prosecution or conviction	—***	—***
Number of Devices		
Detained	409	443

Source: CBP OFO
* Inbound and Outbound
**Border search conducted using external equipment
*** Information not tracked by OFO

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Acting CBP Commissioner
CBP Audit Liaison Office
Office for Civil Rights and Civil Liberties

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Committee on Homeland Security and Governmental Affairs, U.S. Senate
Committee on Homeland Security, U.S. House of Representatives
Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305