~~LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL

# CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities (REDACTED)

**~~Warning: This document is Law Enforcement Sensitive (LES). Do not distribute or copy this report without the expressed written consent of the Office of Inspector General.~~**

~~LAW ENFORCEMENT SENSITIVE~~

**OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

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

July 28, 2020

MEMORANDUM FOR: Mark Morgan
Senior Official Performing the Duties of the Commissioner
U.S. Customs and Border Protection

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

SUBJECT: *CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities – ~~Law Enforcement Sensitive~~*

Attached for your action is our final report, *CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities – ~~Law Enforcement Sensitive~~*. We incorporated the formal comments provided by your office.

The report contains seven recommendations aimed at improving the effectiveness of CBP's covert testing program. Your office concurred with all seven recommendations. Based on information provided in your response to the draft report, we consider recommendation 7 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider recommendations 1 through 6 open and resolved. 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 of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. 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 Sondra McCauley, Assistant Inspector General for Audits, at (202) 981-6000.

Attachment

# DHS OIG HIGHLIGHTS

## *CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities*

**July 28, 2020**

## Why We Did This Audit

The *Trade Facilitation and Trade Enforcement Act of 2015* requires CBP to conduct risk-based covert testing of its operations. We conducted this audit to determine whether CBP's covert tests identify vulnerabilities at ports of entry and borders and whether CBP uses the test results to address identified vulnerabilities and shares lessons learned throughout the component.

## What We Recommend

We made seven recommendations to CBP that, when implemented, should strengthen its covert testing program.

**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

U.S. Customs and Border Protection (CBP) does not comprehensively plan and conduct its covert tests, use covert test results to address vulnerabilities, or widely share lessons learned. In particular, CBP's two covert testing groups do not use risk assessments or intelligence to plan and conduct covert tests at ports of entry and U.S. Border Patrol checkpoints, do not plan coordinated tests, and do not design system-wide tests. This occurred because CBP has not provided adequate guidance on risk- and intelligence-based test planning, directed the groups to coordinate, given them the necessary authority, or established performance goals and measures for covert testing.

Following testing, CBP does not widely share covert test results, consistently make recommendations, or ensure corrective actions are taken. Results are not widely shared because CBP has not defined roles and responsibilities for such sharing. Covert testing groups do not make recommendations or ensure corrective actions are implemented due to insufficient authority and policies directing these actions.

Finally, CBP does not effectively manage covert testing groups to ensure data reliability, completeness, and compliance with security requirements due to leadership changes and limited staff. Without comprehensive planning, incorporating lessons learned from test results, and program management accountability, CBP cannot ensure it addresses vulnerabilities, which may be exploited and threaten national security.

## CBP Response

CBP concurred with all seven recommendations.

## Table of Contents



## Appendixes



## Abbreviations

| | |
|---|---|
| CBP | U.S. Customs and Border Protection |
| CIAP | Checkpoint Internal Assessment Program |
| CPMO | Checkpoint Program Management Office |
| ECD | estimated completion date |
| GAO | U.S. Government Accountability Office |
| OI | Office of Intelligence |
| OIG | Office of Inspector General |
| OFTD | Operational Field Testing Division |
| OFO | Office of Field Operations |
| OPR | Office of Professional Responsibility |
| SOP | standard operating procedure |
| TSA | Transportation Security Administration |

## Background

U.S. Customs and Border Protection's (CBP) mission is to safeguard U.S. borders by preventing illegal movement of people and contraband through land, sea, and air ports of entry, as well as between ports of entry and at interior checkpoints.[1] Two entities within CBP help carry out this mission:[2]

- The Office of Field Operations (OFO) is responsible for operations at ports of entry. OFO Headquarters is composed of seven Executive Directorates that, in turn, include divisions for specific programs and mission segments. Program managers are responsible for oversight of a specific program or mission segment. That responsibility includes policy development, implementation, and maintenance, as well as oversight of training development, equipment functions, and personnel.

- U.S. Border Patrol is responsible for borders between ports of entry. Border Patrol's Checkpoint Program Management Office (CPMO) is part of the Law Enforcement Operations Directorate and assists in addressing checkpoint policy issues as well as reviewing checkpoint performance measures.

To safeguard U.S. borders, CBP uses a multi-layered enforcement strategy, which incorporates a variety of tools and techniques for customs, immigration, border security, and agricultural protection. CBP established two groups responsible for covert testing to evaluate the effectiveness of OFO's and Border Patrol's implementation of this strategy. Specifically:

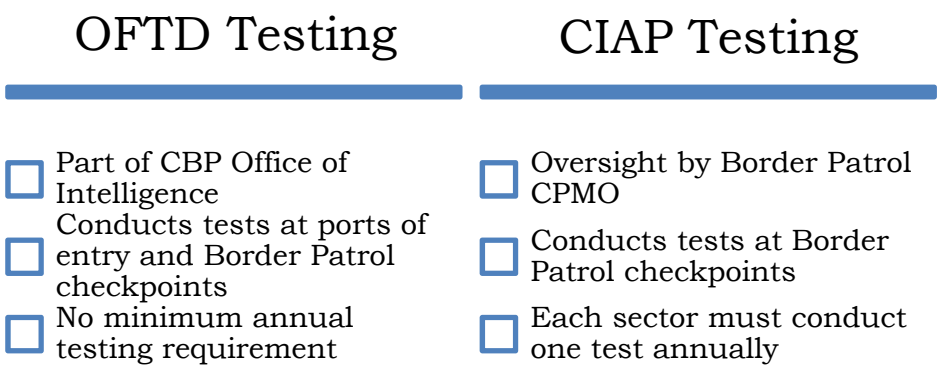
- CBP's Operational Field Testing Division (OFTD) conducts covert testing operations at U.S. ports of entry and border checkpoints.
- Border Patrol's CPMO oversees the Checkpoint Internal Assessment Program (CIAP), which requires Border Patrol sectors with permanent checkpoints to conduct annual internal assessments (covert tests).

CBP uses these covert test groups at OFO ports of entry and Border Patrol checkpoints to identify compliance issues and vulnerabilities related to use of

[1] Border Patrol operates checkpoints within 100 miles of the U.S. border as part of its multilayered enforcement strategy. During a checkpoint stop, officers may question vehicle occupants about their citizenship, request proof of immigration status, and observe what is in plain view inside a vehicle. Border Patrol maintains permanent and temporary checkpoints in nine sectors along the Southwest border.
[2] A third entity, CBP's Air and Marine Operations, deploys aircraft and maritime vessels to provide rapid air and marine response capabilities. It has not been subject to covert testing and is outside the scope of this audit.

fraudulent documents, smuggling of illegal aliens and goods, nuclear and radiation threats, and use of facial recognition technology. Figure 1 provides a comparison of OFTD's and CIAP's organizational placement and scope of covert testing.

**Figure 1: Comparison of CBP Covert Testing Groups**




*Source:* OIG analysis of CBP records

**OFTD Covert Testing**

In 2007, CBP established OFTD under the Office of Professional Responsibility (OPR) to address requirements of the *Security and Accountability for Every (SAFE) Port Act of 2006* (Safe Port Act). The Safe Port Act requires CBP to covertly test radiation detection capabilities.

Since 2007, OFTD has expanded to conduct covert testing at U.S. ports of entry and border checkpoints. In 2014, the U.S. Government Accountability Office (GAO) reported OFTD had not prioritized covert operations testing based on assessed risks.[3] GAO also found OFTD did not track corrective actions to address vulnerabilities identified by covert testing. In 2014, CBP moved OFTD from OPR to its Office of Intelligence (OI). As of August 2019, OFTD had 10 full-time staff, supplemented by approximately 30 detailees from various CBP offices, and a covert testing budget of about $300,000 per year for travel.

According to OFTD, it plans and conducts covert tests at ports of entry or border checkpoints based on requests and priorities from operational entities. For some covert tests, OFTD staff go to ports or checkpoints several days or weeks in advance to gather information on the location and mitigate challenges to test execution. Using this information, OFTD collaborates with OFO or Border Patrol to design scenarios for the assessment.

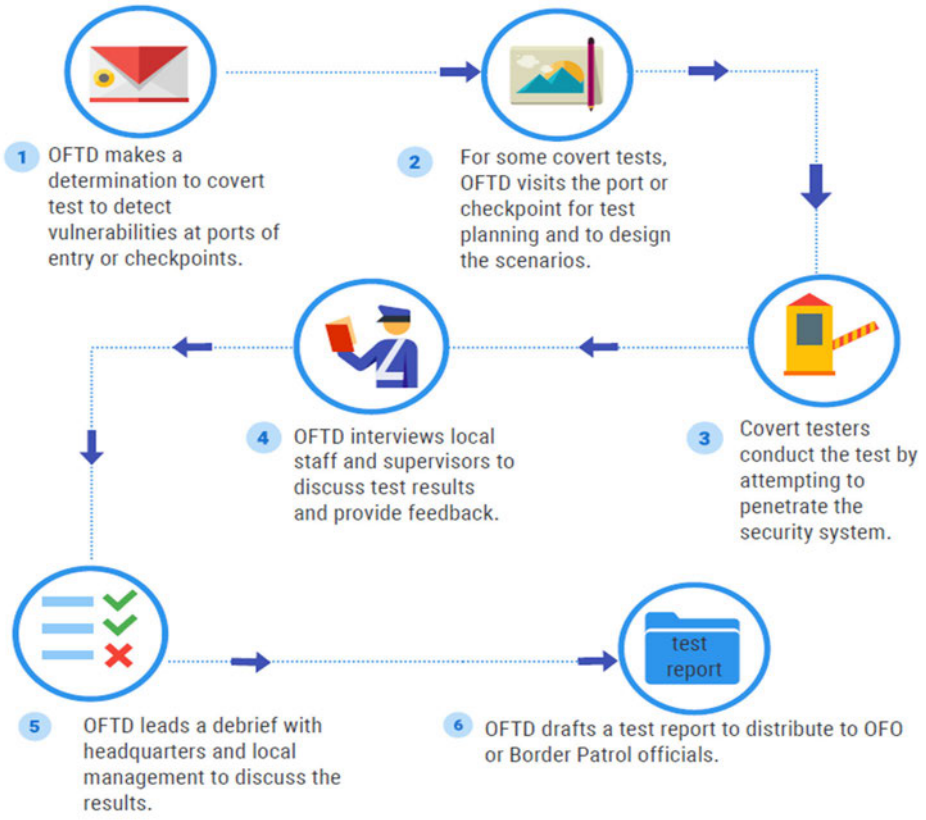
[3] *Combatting Nuclear Smuggling – Risk Informed Covert Assessments and Oversight of Corrective Actions Could Strengthen Capabilities at the Border* (GAO-14-826), September 2014.

When conducting covert tests, OFTD staff, assisted by detailed CBP employees, act as role players and attempt to penetrate security systems at ports of entry or border checkpoints, using fraudulent documents, illegal items, or other techniques. Role players may conduct multiple tests at a single location on the same day.

After some tests, OFTD interviews the CBP officers involved, as well as local supervisors, to discuss results and provide feedback on the testing process.[4] OFTD staff also lead de-briefs with OFO field office or Border Patrol sector management, as well as OFO's Integrity Center[5] or Border Patrol's CPMO, to discuss the covert tests results. Upon completion of the tests, OFTD analyzes results and prepares test reports. It reports whether CBP officers and agents were successful in detecting (interdicting) the illicit persons or items during the test. OFTD distributes reports to the Integrity Center or selected officials at Border Patrol headquarters, and also sometimes sends results to Border Patrol sector leadership. Figure 2 provides a flowchart of OFTD's process for conducting covert tests.

[4] OFTD has five standard operating procedures for covert testing, which have different requirements for interviewing CBP officers and supervisors involved in the tests. OFTD may not want to break its covert character so it can continue to conduct additional tests.
[5] OFO's Integrity Center serves as the OFO liaison to OFTD and OPR.

**Figure 2: OFTD Covert Testing Process**




*Source:* OIG analysis of observations, OFTD documentation, and interviews

**Border Patrol Covert Testing under CIAP**

Separate from OFTD, Border Patrol conducts covert testing at checkpoints as part of CIAP, established in 2014. CPMO oversees CIAP, which has a standard operating procedure (SOP) requiring Border Patrol sectors with permanent checkpoints to conduct annual internal covert tests on detecting fraudulent documents, imposters, radiation, and other areas. In addition to these annual tests, sector leadership has the flexibility to direct other checkpoint tests it deems necessary. Sector staff must also establish their own processes for conducting covert testing.

We conducted this audit to determine whether CBP's covert tests identify vulnerabilities at ports of entry and borders and whether CBP uses the test results to address identified vulnerabilities and shares lessons learned throughout the component.

## Results of Audit

CBP does not comprehensively plan and conduct its covert tests, use covert test results to address vulnerabilities, or widely share lessons learned. In particular, CBP's two covert testing groups do not use risk assessments or intelligence to plan and conduct tests at ports of entry and Border Patrol checkpoints, do not plan coordinated tests, and do not design system-wide tests. This occurred because CBP has not provided adequate guidance on risk- and intelligence-based test planning, directed the groups to coordinate, given them the necessary authority, or established performance goals and measures for covert testing.

Following testing, CBP does not widely share covert test results, consistently make recommendations, or ensure corrective actions are taken. Results are not widely shared because CBP has not defined roles and responsibilities for such sharing. Covert testing groups do not make recommendations or ensure corrective actions are implemented due to insufficient authority and policies directing these actions.

Finally, CBP does not effectively manage covert testing groups to ensure data reliability, completeness, and compliance with security requirements due to leadership changes and limited staff. Without comprehensive planning, incorporating lessons learned from test results, and program management accountability, CBP cannot ensure it addresses vulnerabilities, which may be exploited and threaten national security.

### CBP's Covert Testing Groups Do Not Adequately Plan, Coordinate, or Design Tests to Identify Systemic Vulnerabilities

CBP's two covert testing groups do not use risk assessments or collaborate with intelligence partners to plan and conduct tests that identify weaknesses throughout CBP. The testing groups also do not coordinate with each other to plan tests that prevent duplication of effort. Finally, the groups primarily design tests for single ports or sectors rather than planning repeatable tests for multiple locations, which would help identify systemic vulnerabilities.

**CBP's Covert Testing Groups Do Not Use Risk Assessments or Intelligence to Plan Covert Tests and Do Not Plan Coordinated Tests**

According to the *Trade Facilitation and Enforcement Act of 2015*, CBP's OI is required to conduct risk-based[6] covert testing. Additionally, DHS' *Integrated Risk Management* directive requires components to use risk to inform decision-making processes and DHS' *Risk Management Fundamentals* recommends documenting that process. Despite these requirements, we found that CBP's covert testing planning process is informal and undocumented and does not connect to risk assessments or senior leadership priorities. Additionally, CBP testing groups do not coordinate to prevent duplication.

Risk and Intelligence Not Used in Test Plans

OFTD does not use risk assessments to plan covert tests. In 9 of 10 test operations plans with 21 test scenarios we reviewed, OFTD did not document the risk-based rationale for choosing the test types or locations. Instead, the operations plans covered logistics, such as travel information and local points of contact. One operation plan we reviewed was for a location highlighted in an OFTD-created report ranking seaport risks, but the plan did not connect the rationale for choosing that location with the report.

Further, although CBP produces annual priorities documents, OFTD could not provide any intelligence-based risk assessment that connected testing to OFO or Border Patrol priorities.[7] From FY 2016 through FY 2018, OFTD produced one risk assessment at the request of the OI Assistant Commissioner. Specifically, in 2017, in conjunction with representatives of the Australian Border Force, OFTD provided an intelligence assessment of operations at the Miami port and risks to the cruise industry. However, we could not connect any of OFTD's subsequent testing activities to the priorities identified by the risk assessment. OFTD officials acknowledged that the risk assessment was not a typical product for them and they did not use it to direct testing. The office also does not have plans to produce that type of risk assessment in the future.

[6] The DHS Lexicon defines risk-based decision making as determining a course of action predicated primarily on assessment of risk and the expected impact of the course of action on that risk.

[7] On an annual basis, the CBP Commissioner issues priorities for the organization. Each division produces priorities based on this to achieve the Commissioner's priorities. For example, in FY 2019, the Commissioner set as a priority increasing the number of applicants for CBP positions and improving the efficiency of the hiring process. In response, the Chief of Border Patrol set as a priority increasing recruitment of Border Patrol agents in areas farther from the border.

OFTD also could not demonstrate it prioritized tests based on available intelligence.[8] In particular, OFTD did not collaborate with intelligence divisions within OI to produce overall risk assessments that aligned testing with high-risk areas. For example, in the summer of 2018, OFTD planned and conducted a series of [redacted] smuggling tests across the Southwest border[9] without documenting the risk- or intelligence-based rationale. According to its report summarizing the test results, OFTD requested information from OI after it completed the tests, only to confirm that the test scenario had a basis in intelligence. Although OFTD is part of OI, OI Division Directors with responsibility for analyzing intelligence across CBP said they had limited to no interaction with OFTD. Those OI Division Directors also did not provide intelligence to OFTD for test planning or receive test results from OFTD to inform their intelligence products.

Like OFTD, Border Patrol did not prepare risk or intelligence assessments or document the rationale for the types of tests conducted. CPMO did not provide any guidance to sectors on how to conduct tests. Instead, Border Patrol sector leadership independently chose the types of tests to conduct and which checkpoints to test, based on its preferences for type or location of the test.

CBP has not used risk or intelligence assessments to plan testing because neither OI nor the Border Patrol Law Enforcement Operations Directorate has provided sufficient guidance to their respective covert testing groups. OI has provided minimal guidance to OFTD on how to carry out Congress' mandate to conduct risk-based covert testing. Although OI leadership provided office-wide priorities that, on some occasions, included covert testing, it has not provided any additional written guidance to OFTD on how to achieve its mission or fulfill its responsibility to conduct intelligence-based covert testing. Border Patrol's Law Enforcement Operations Directorate also has not provided written guidance. Although the CIAP SOP empowers Border Patrol sectors to conduct covert tests, it does not require sectors to plan based on intelligence or coordinate with Border Patrol's intelligence unit.

[8] In this report, intelligence refers to information of tactical, operational, or strategic value.
[9] The series of tests consisted of a scenario in which a single occupant (driver) of a mini-van or SUV proceeded through a checkpoint attempting to smuggle [redacted].

Limited Test Planning Coordination

In addition to not using risk or intelligence assessments to plan tests, testing groups do not coordinate with each other. OFTD does not always coordinate with Border Patrol during their respective planning phases to prevent duplication of effort. Border Patrol sectors do not coordinate their test plans with other sectors because each sector can develop its plan based on sector-specific issues.

Although it would prevent duplication of effort, the two groups have not coordinated because CBP leadership has not directed them to do so. Further, Border Patrol does not coordinate with OFTD on covert test types or locations as its leadership does not believe sectors and ports of entry face the same threats. To enhance coordination, Border Patrol provided detailees to OFTD. However, this has not happened consistently, even though both OFTD and Border Patrol leadership agreed that without detailees, coordination decreased.

**CBP Does Not Plan Repeatable Covert Tests at Multiple Locations to Identify Systemic Vulnerabilities**

CBP does not plan system-wide covert tests to detect broad-based vulnerabilities. For an example of how to plan such tests, we examined policies and procedures of the Transportation Security Administration's (TSA) covert testing group, which develops project plans to direct series of tests. TSA's process allows testers to use the same test scenario at multiple locations to determine whether a weakness, and thus a threat, exists throughout the component. TSA's SOP requires detailed project plans that include the purpose of the testing project, the threat item, scenario, and the test methodology. The procedures also typically require sections for assumptions, deliverables, milestones, and a testing schedule. Although they could benefit the component, neither CBP testing group plans or conducts repeatable, systemic covert tests.

OFTD does not plan or conduct CBP-wide, systemic testing. We reviewed 10 OFTD operations plans and found that none included such testing. Additionally, only 1 of the 10 operations plans included testing at more than 1 field office or sector. For example, in 2016, OFTD planned [redacted] testing at four checkpoints in the El Paso Sector, but did not include any plans for conducting this same test at other locations throughout CBP. OFTD also did not report it conducted follow-up testing to assess improvement from any prior test results in any of the operations plans. Finally, OFTD has not written any project plans, or similar documents, detailing testing purpose, scope, and methodology for series of tests.

Although program managers responsible for making OFO-wide policy changes said testing at multiple locations might help identify systemic threats, OFTD does not use risk assessments or strategically plan such tests. Instead, according to OFTD leadership, they choose some test locations based on requests from ports of entry and others based on the CBP Commissioner's priorities, OFO or Border Patrol requests, and budget. OFTD's database shows that, from FY 2016 through FY 2018, OFTD conducted 332 different tests.[10] However, during this timeframe, OFTD produced two summary reports — one in 2018 about [redacted] smuggling tests conducted across the Southwest border, which analyzed trends across multiple sectors, and another evaluating multiple non-intrusive inspection tests conducted in a single field office. These types of tests can provide valuable information about systemic vulnerabilities. For example, in the 2018 [redacted] smuggling tests of a single threat at Southwest border checkpoints, OFTD found agents interdicted [redacted] in only [redacted] percent of covert tests.

For their part, Border Patrol sectors also do not plan systemic testing. Instead, sector leadership directs testing within their individual sectors. Additionally, CPMO did not conduct any analysis of sector test results to identify trends or common issues.

OFTD and CPMO do not plan or conduct repeatable tests because neither CBP nor the leadership for the groups has given them the necessary authority to do so. First, OFTD has no signed directive describing its authority for conducting tests or procedures requiring it to plan risk-based, systemic covert tests. Senior OI officials stated that OFTD does not have permission to test scenarios without the consent of OFO and Border Patrol. Therefore, OFTD relies on the cooperation of OFO and Border Patrol to plan and conduct tests. For example, following interdiction failures in biometrics and agriculture testing[11] at the [redacted] International Airport, senior program officials from OFO's Agriculture Program and Trade Liaison said they told OFTD they had other testing priorities and did not want to test the agriculture scenario further. As a result, OFTD stopped testing the scenario. Although OFTD leadership drafted an *Operational Field Testing (Red Teaming)* directive in March 2019, the directive did not clarify OFTD's authority to independently test. For example, it does not clearly define organizational independence and

[10] See page 18 for discussion about OFTD's incomplete database.
[11] OFTD conducted biometric covert testing to determine whether CBP's biometric [redacted] would detect [redacted] and whether CBP officers would correctly [redacted]. OFTD conducted agriculture testing to determine whether CBP agriculture specialists would intercept suspicious items and [redacted].

does not emphasize independence in areas of planning and conducting tests. Second, CPMO does not have authority to plan testing scenarios to identify high-risk systemic weaknesses across Border Patrol sectors, coordinate sector covert testing, or direct sector test plans. Border Patrol's CIAP SOP describes requirements for sectors to conduct tests, but does not describe how sectors are to select and plan tests. The document that established CPMO also does not provide authority to direct or coordinate system testing.[12]

In addition, testing groups are not conducting systemic tests because CBP has not established specific performance goals or measures that covert testing groups should accomplish or demonstrate. For example, when asked how OI measures OFTD's performance, senior leaders stated they measured OFTD's success not by security gaps identified by OFTD and closed by OFO and Border Patrol, but rather OFO's and Border Patrol's willingness to cooperate with OFTD.

## CBP Does Not Share Test Results, Make Recommendations, or Ensure Corrective Actions Are Taken

Once covert tests are completed, OFTD, CPMO, and OFO do not widely share test results or lessons learned across CBP, including with leadership of other Border Patrol sectors and OFO field offices or with CBP intelligence officials. Additionally, neither the OFTD nor the Border Patrol covert testing group consistently makes recommendations. In the limited instances in which they make recommendations, neither group ensures that OFO and Border Patrol take corrective actions to resolve the local vulnerabilities identified. CBP also does not track the implementation of such actions.

### CBP Does Not Share Test Results Across the Organization

According to GAO's *Standards for Internal Control in the Federal Government,* organizational leadership should establish reporting lines, ensure information is communicated throughout the organization, and assign responsibilities to achieve objectives and address related risks. As an example of communicating information throughout an organization, TSA shares vulnerabilities it identifies during covert testing through a process that ensures component-wide visibility and evaluation of the vulnerabilities.[13] In contrast to TSA, and although it would help CBP identify and evaluate vulnerabilities component-wide, neither

[12] *Implementation of Checkpoint Program Management Office,* memorandum from U.S. Border Patrol Chief Michael J. Fisher, July 8, 2013.
[13] *TSA Improved Covert Testing but Needs to Conduct More Risk-Informed Tests and Address Vulnerabilities* (GAO-19-374), April 2019.

testing group consistently shares the results of testing with sector and field office leadership, intelligence officials, or across the organization.

OFTD does not consistently share test results. When we attempted to identify with whom OFTD shared results, we found OFTD also did not routinely maintain documentation on who received its test results. For example, OFTD could not find report distribution records for 8 of 21 test scenarios conducted in FY 2016 through FY 2018. OFTD uploaded another 10 of the 21 test scenario results to a shared folder, but could not identify who had access to that folder. For the remaining three test scenarios, OFTD produced emails demonstrating that it shared its test reports with some officials, but none of these reports showed that OFTD distributed them to multiple field offices or sectors. According to OFTD officials, they sent report results to a limited number of headquarters personnel and some Border Patrol sector leadership whom they thought were directly impacted by testing.

In multiple discussions, OFO program managers confirmed they were unaware of OFTD testing or the results. In some cases, the managers knew about testing from oral debriefings, but they did not always receive written test reports because they were not widely shared. For example, OFTD conducted biometric and agricultural covert testing at [redacted] International Airport in November 2018. In February 2019, OFTD transmitted the test report with results to the OFO Integrity Center, which acts as the OFO liaison to OFTD and OPR.[14] However, the OFO Integrity Center only sent the test results to airport officials approximately 2 weeks later — after we requested verification it had distributed the results. Even then, the Integrity Center limited transmission of the report to officials at [redacted] International Airport. It did not send the report to other stakeholders. Agriculture program officials did not receive draft or final copies of the report with the results, while biometric program officials received a copy of the draft report, but did not receive a copy of the final report results. CBP officials in [redacted] said they sent the results to only a narrow group of senior port officials in their field office.

Border Patrol also does not widely share test results. As required by the CIAP SOP, Border Patrol covert testers send results to CPMO, but after previous officials left the office, there were no historical records or a shared folder for the office to centrally store test results. Therefore, to respond to our audit inquiries, CPMO had to request records from each sector. In addition, according to CPMO officials, Border Patrol covert testing groups send CIAP test results to their own sector leadership, but Border Patrol does not require

[14] This distribution delay may have been affected by a lapse in appropriations from December 22, 2018 to January 25, 2019, when non-essential Federal employees were not working.

sectors to share results or lessons learned with other sectors. CPMO could not identify any test results shared with other sectors and had no policy encouraging or requiring sectors to do so.

Test results are not shared because CBP has not established roles and responsibilities for such sharing. OI, OFO, and Border Patrol do not require sharing test results and could not provide any directives or SOPs with a process for doing so. According to CBP leadership, sharing results with a wide audience may increase the risk of operational security information ending up in the wrong hands. Although it may be unnecessary to share test results with all levels of staff, CBP diminishes the impact of covert testing by not communicating this information to senior officials across the organization.

**CBP Does Not Consistently Recommend or Implement Corrective Actions**

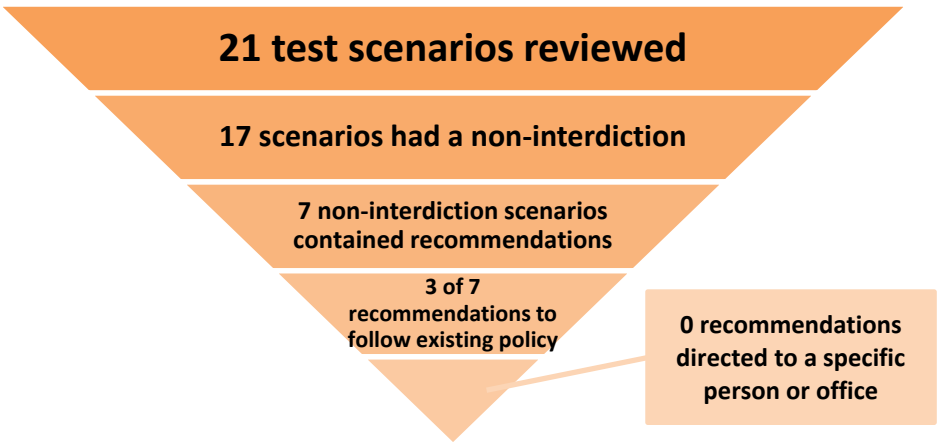
GAO's *Standards for Internal Control in the Federal Government* direct management to complete and document corrective actions to repair internal control deficiencies promptly. Contrary to this guidance, neither of CBP's testing groups consistently makes recommendations for corrective actions. In addition, when recommendations are made, CBP does not ensure corrective action plans are created and implemented.

Inconsistent Recommendations by Both Testing Groups

As of February 2020, according to its covert testing SOPs, OFTD is responsible for recommending corrective actions to address identified vulnerabilities to CBP senior leadership. Although required by its SOPs, OFTD did not always recommend corrective actions based on results of tests conducted from FY 2016 through FY 2018. Of the 21 test scenarios we reviewed, 17 resulted in at least one non-interdiction,[15] but OFTD only made recommendations in 7 of these scenarios (41 percent). In three of the seven scenarios, OFTD's recommendations were restricted to reiterating that program offices should follow existing policies. For example, according to one test recommendation, "when conducting a baggage exam, open the bag fully and conduct a 100% inspection of bags." In none of the seven scenarios did OFTD specifically direct the recommendations to any person or office to take corrective action. Figure 3 shows our analysis of OFTD's limited recommendations in the 21 test scenarios we reviewed.

[15] For this report, non-interdiction refers to CBP's inability to interdict or detect the tester or test item during a scenario.

**Figure 3: OFTD Recommendations Limited in Number and Content**




*Source:* OIG analysis of selected OFTD test scenarios

Although CIAP requires Border Patrol sectors to use covert testers to complete tests, identify weaknesses, and provide guidance in reducing or mitigating risks, Border Patrol testers also did not consistently make recommendations based on non-interdictions. Specifically, from FY 2016 through the third quarter of FY 2018, there were 84 CIAP tests with non-interdictions, but Border Patrol testers did not make recommendations after conducting 6 of those tests.

No Assurance Corrective Actions are Created and Implemented

In addition to inconsistent recommendations, when recommendations are made, CBP does not ensure corrective action plans are created and implemented and does not hold appropriate senior officials accountable for addressing vulnerabilities. Neither OFO nor Border Patrol demonstrated they consistently took corrective actions after non-interdictions during tests, even though CBP describes detection and interdiction as key duties for Border Patrol agents and the mission of OFO's inspection program. For example, OIG reported in a 2018 audit of CBP's Global Entry program that, in 18 percent of covert tests conducted by OFTD from FY 2010 to FY 2017, testers successfully entered the United States using fake Global Entry receipts.[16] During the same audit, at a sample of airports, we observed the same vulnerability in the Global Entry process.

Although not formally assigned this responsibility, the OFO Integrity Center assumed responsibility for facilitating and tracking corrective actions following OFTD covert testing. The Integrity Center had only 1 OFO corrective action

[16] *CBP's Global Entry Program is Vulnerable to Exploitation* (OIG-19-49), June 2019.

plan from FY 2018, even though in 46 tests, 19 non-interdictions were identified.[17] Integrity Center officials said they believed some of the non-interdictions in FY 2018 did not warrant corrective actions. For the corrective actions the Integrity Center tracks from prior years, it does not request any records to verify corrective actions OFO field offices implement. Integrity Center officials also said they do not direct any timelines for corrective action implementation and just document what OFO program managers commit to doing.

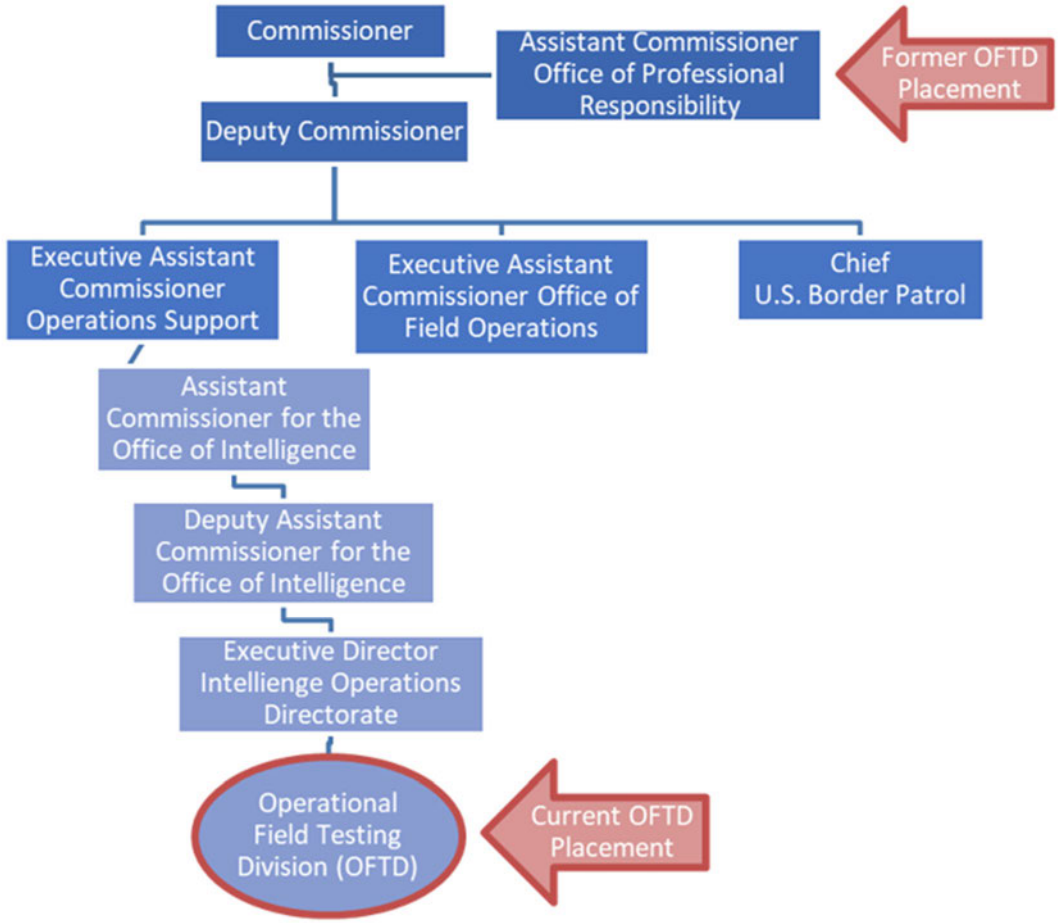
Despite CBP reporting interdictions between ports of entry on the Southwest Border as a key strategic measures of effectiveness,[18] Border Patrol did not have any corrective action plans for 44 OFTD tests at checkpoints with non-interdictions.[19] CPMO also had no records of corrective action plans for non-interdictions noted in Border Patrol tests conducted between FY 2016 and FY 2018.[20]

Insufficient Authority and Policies

OFTD made inconsistent recommendations and did not ensure corrective actions were implemented because the office does not have sufficient authority. Officials who oversee OFTD said that, contrary to its SOPs, they do not believe OFTD has the authority to make recommendations. OFTD senior officials said their reports should include observations and findings, but not recommendations, and stated they did not feel qualified to recommend corrective actions or ensure they are implemented. The officials explained that when within OPR, OFTD had enforcement power, and the operational entities perceived covert testing as punitive. In addition, as part of OPR, they reported directly to and briefed the CBP Commissioner. Now, as part of OI, OFTD's relationship with operational entities is more collaborative — it has no enforcement power and officials no longer brief the Commissioner. Figure 4 shows the difference between OFTD's former and current placement.

[17] See page 18 for discussion of OFTD's incomplete database.
[18] In FYs 2016 through 2020, CBP reported results in key measures, including interdictions between ports of entry on the Southwest Border, to demonstrate progress towards its strategic goals by mission programs, as required by the *GPRA Modernization Act of 2010*, P.L. 111-352. See *Department of Homeland Security, U.S. Customs and Border Protection, Budget Overview, Fiscal Years 2016-2020, Congressional Justification.*
[19] OFTD's database included 82 Border Patrol tests from FY 2016 through FY 2018 and listed 44 of these tests as non-interdictions. However, later in this report, we note that OFTD's database was incomplete and specifically missing Border Patrol test records.
[20] Due to differences in how each sector aggregates and reports information, we could not estimate a total of non-interdictions for the CIAP program in this timeframe.

**Figure 4: CBP Organizational Chart Showing OFTD Placement**




*Source:* OIG analysis of CBP organizational chart

OFO and Border Patrol do not create and implement corrective action plans due to insufficient policies. For OFO, the Integrity Center said it requests corrective action plans from the OFO field office following a test. For example, after the FY 2019 [redacted] covert tests, the Director of Field Operations and Port Director sent short-term and long-term goals for corrective action to the Integrity Center. Although Integrity Center officials said they typically follow up each quarter on pending actions and did so in February 2019, OFO does not have a policy formalizing covert testing responsibilities.

For Border Patrol testing, CIAP policy does not specify any requirements for implementing corrective actions, and CPMO has no authority to enforce corrective action implementation. According to CPMO, sector leadership is responsible for ensuring sectors take corrective actions. As a result of our audit, CPMO began developing a new directive to clarify its authority and

procedures, as well as a database to centralize test results and track corrective actions taken by sectors.

## CBP Does Not Effectively Manage Covert Testing Groups to Ensure Test Data Reliability, Completeness, and Compliance with Security Requirements

The *GPRA Modernization Act of 2010* requires each agency to establish a strategic plan with general goals and objectives and describe how it will ensure the reliability of the data used to measure progress toward its goals. In addition, according to GAO's *Standards for Internal Control in the Federal Government*, management should use quality information that is complete to achieve an organization's objectives. Finally, *Executive Order 13526 – Classified National Security Information* requires a uniform system for safeguarding and classifying national security information, including specific classified markings.[21] Contrary to this guidance, we found that CBP does not manage its covert testing groups to ensure data reliability, completeness, and compliance with security requirements.

### Ineffective OFTD Management

OFTD did not take steps to ensure data reliability and completeness; instead, among other actions, it arbitrarily excluded test results and did not report non-interdictions during tests to CBP officials for awareness and corrective action. For example, we observed OFTD covert testing at [redacted] International Airport and identified instances when OFTD did not report all test results. Specifically, OFTD conducted a series of biometric covert tests using similar scenarios, but excluded the results for 5 of the 10 tests in its summary report. Officials said they excluded the results of three tests because the biometric system was inoperable and, therefore, these tests could not be completed using the planned scenario. However, OFTD also excluded non-interdiction results from two tests that occurred when the biometric system was operational. According to OFTD officials, they excluded the non-interdiction results from the two tests because they were using that scenario to collect data rather than test. Despite this assertion, before conducting the tests and in an advance briefing to a senior OFO official, OFTD included these as tests and not data collection efforts. Therefore, we believe the results were valid and also counted them as tests.

Further, before testing began, OFTD did not have a policy with rules for including or excluding test results. Therefore, the subsequent reports did not

[21] *Classified National Security Information,* Executive Order 13526, December 29, 2009.

document the reasons for excluding any of the results of the five tests. Not establishing such rules in advance of testing makes it more difficult for OFTD to confirm the validity of overall test results and avoid results that appear skewed or "cherry-picked." For example, biometric program officials requested that OFTD not test the scenario mentioned above where two test results were excluded because they were concerned the biometric software would likely fail the test. Although OFTD conducted the test, it excluded the results, making it appear OFTD wanted to show more positive results.

Further, at the time of our fieldwork, OFTD's database of covert testing results was incomplete. For example, we reviewed OFTD's [redacted] smuggling summary report and verified that, between May and August 2018, OFTD conducted 119 smuggling tests in 9 locations. However, the office's database reflected only 25 [redacted] smuggling tests in 3 locations during this timeframe, meaning OFTD entered just 21 percent of tests into the database. Further, the database included the count of test interdictions by operational entity, but did not include associated test reports, findings, recommendations, or corrective actions, as required by OFTD's SOP. OFTD staff said they used the database primarily to generate sequential test identification numbers. Although OFTD is developing a new database to document required information and identify trends to improve the testing process, staff did not know when they would start using it.

OFTD also did not ensure its reported test results complied with security requirements. We reviewed 31 test reports marked classified by OFTD staff. All reports were missing some paragraph markings to indicate which sections of the document were classified, and 26 of the reports were missing classification blocks describing the author, classification authority, and declassification date. We could not determine whether supervisors reviewed reports prior to their dissemination because the reports were unsigned and undated. Further, OFTD officials could not specify why they classified the documents nor could they provide the classification guide they had used. We reported this to CBP's point of contact for security classification issues, located in CBP OPR, who later determined OFTD had over-classified the documents.

**Ineffective Border Patrol Management**

Border Patrol also did not take steps to ensure data reliability and completeness. Before our fieldwork concluded in August 2019, CPMO also did not have reliable data for providing or using covert test results. Specifically, at that time, CPMO had no centralized database to track test results or corrective actions. In August 2019, however, CPMO demonstrated that it had implemented a database to record CIAP test results.

CPMO did not ensure required covert tests were conducted and that it maintained complete records. Prior to our audit, CPMO did not record or track which Border Patrol sectors conducted required CIAP covert tests. In reviewing all test reports sector covert testers produced, we determined that, from the program's implementation in 2014 until the beginning of our audit in June 2018, three of nine sectors did not conduct any CIAP tests. A senior CPMO official explained that some checkpoints were not aware of the CIAP covert testing requirement and, as a result, these sectors did not conduct any tests. Although we identified six sectors that developed their own CIAP covert testing SOPs, CPMO did not help those sectors create SOPs to ensure consistency or compliance with the program requirements.

**Leadership Changes and Limited Staff**

We attribute CBP's ineffective management of OFTD and CPMO data and security compliance to multiple leadership changes at OI and CPMO and limited staff with competing priorities. Specifically, OFTD has had multiple directors and acting directors since its move to OI, which inhibited its ability to develop SOPs. Attempting to fill multiple roles limits time to complete all leadership and supervisory tasks, such as drafting and issuing procedures for data reliability and completeness, as well as providing supervisory review of reports for completeness and correct security markings. CPMO also experienced multiple leadership changes. Due to limited tenure in their positions, prior leaders did not establish any common shared drives or databases to track information and had no policies to ensure data was reliable and complete. Although OFTD had requested funding to develop a database, OI did not fund those requests until FY 2018. CPMO did not recognize a need to develop data from its covert testing until we pointed it out as part of our audit.

At the conclusion of our fieldwork in August 2019, both groups were developing policy documents, but they were in draft and leadership had not approved or implemented them. Although CPMO has since provided us with an approved, implemented policy with improvements in defining which data to report and supervisory review, the policy does not address data quality monitoring.

## Conclusion

Effective covert testing is an essential part of a multi-layered strategy for guarding against dangerous people and materials that continue to threaten our national security. Without incorporating analysis of the risks and conducting comprehensive testing at ports of entry and U.S. borders, unknown threats and vulnerabilities may persist. Without authority, clear direction, and

performance measures to plan and conduct risk-based, systemic testing, CBP's covert testing groups will not be able to provide agency leadership with an independent, unbiased assessment of whether its programs operate effectively to meet its mission.

CBP also diminishes the impact of covert testing by not sharing test results with senior officials across the organization, not consistently making recommendations, and not tracking corrective actions to ensure they are implemented. As a result, similar vulnerabilities across ports of entry and border checkpoints may remain unaddressed. Finally, the absence of reliable and complete test data prevents CBP from identifying trends and may lead to a waste of resources. Until CBP addresses these issues, weaknesses at our borders may continue to be exploited.

## Recommendations

**Recommendation 1:** We recommend that the Deputy Commissioner of CBP develop and implement policies to ensure CBP's covert testing groups:

a. develop risk-based annual covert test plans and identify systemic tests;
b. distribute test results throughout the organization;
c. make recommendations; and
d. implement and track corrective actions.

**Recommendation 2:** We recommend that the Deputy Commissioner of CBP study the effectiveness of maintaining multiple covert testing groups, and if CBP maintains multiple groups, we recommend specifying roles, responsibilities, and requirements for coordination to eliminate redundancies.

**Recommendation 3**: We recommend that the CBP Executive Director of Policy assign roles and responsibilities for planning and conducting covert tests, making recommendations, and overseeing corrective actions.

**Recommendation 4:** We recommend that the Deputy Commissioner of CBP:

a. assess organizational placement and resources of Operational Field Testing Division to determine the best placement in CBP's organizational chart, and
b. provide OFTD authority to plan and conduct independent, system-wide tests, make recommendations, and track corrective actions.

**Recommendation 5:** We recommend that the Assistant Commissioner of Office of Intelligence and Border Patrol's Chief of Law Enforcement Operations Directorate direct covert testing entities to develop and implement both performance measures and standard operating procedures including:

a. processes for determining data to be included in test reports,
b. data quality monitoring, and
c. supervisory review.

**Recommendation 6:** We recommend that the Assistant Commissioner of Office of Intelligence and Border Patrol's Chief of Law Enforcement Operations Directorate direct covert testing entities to develop and implement databases to record test results, recommendations, and the status of corrective actions.

**Recommendation 7:** We recommend that the Assistant Commissioner of the Office of Intelligence direct all Operational Field Testing Division staff to review all prior and future classified reports to ensure they are properly marked to protect national security information.

**OIG Analysis of DHS Comments**

We obtained written comments on a draft of this report from the CBP Senior Component Accountable Official. CBP concurred with all seven of our recommendations. We have included a copy of the comments in their entirety in appendix B. We also received technical comments and revised the report as appropriate. Following is our evaluation and response to CBP's comments.

**OIG Response to General Comments:**

In its response to the draft report, CBP expressed concern that the OIG's report contains several inaccurate representations, including the definition of "risk" applied to CBP's testing methodologies. CBP asserted its senior managers drive the component's covert testing activities to identify unknown risk versus known risk. The results of these tests inform its risk assessments instead of using risk assessments to inform covert testing. However, we do not agree this methodology meets the risk-based testing requirement of the *Trade Facilitation and Trade Enforcement Act of 2015*. Further, the DHS Risk Lexicon defines risk-based decision making as determining a course of action predicated primarily on the assessment of risk and using the assessment of risk as the primary decision driver.

CBP also asserted that its covert test groups do not measure operational success by detection and interdictions. This statement conflicts with what CBP reports as key responsibilities for its staff, as well as factors CBP uses to support its annual budget requests. CBP describes one of the most important duties of a Border Patrol agent as detecting and apprehending terrorists, undocumented aliens, and smugglers of aliens at or near the land border. OFO reports similar duties for its inspection program, including preventing smuggled agricultural products. CBP also reports the rate of interdiction effectiveness along the Southwest border between ports of entry as one of five key measures to demonstrate progress toward its strategic goals,[22] as required by the *GRPA Modernization Act of 2010*. As such, the importance of interdictions at CBP is clear. It is further reinforced by covert test groups that report their test interdiction rates internally.

[22] *Department of Homeland Security, U.S. Customs and Border Protection, Fiscal Year 2020, Budget Overview, Congressional Justification*, pp. 6-7.

Nonetheless, we recognize the actions CBP stated it has taken to increase its system-wide testing. Specifically, CBP stated that OFTD conducted four series of system-wide tests with OFO and Border Patrol in FY 2019, which occurred after the scope of our review of OFTD's covert test reports.

**CBP Comments to Recommendation 1:** Concur. Once Operations Support, in collaboration with OI and Border Patrol, determines the effectiveness of maintenance and placement of multiple covert testing groups, CBP will develop standard operating procedures for risk-based testing. Estimated completion date (ECD): April 30, 2021.

**OIG Analysis of CBP Comments:** CBP's proposed actions are responsive to the recommendation. We consider this recommendation resolved and open. It will remain open until CBP provides documentation of its new covert testing standard operating procedures.

**CBP Comments to Recommendation 2:** Concur. Operations Support, in collaboration with OI and Border Patrol, will form a working group to study the effectiveness of maintaining multiple covert testing groups within CBP and present results to the Deputy Commissioner. The presentation will include proposed assignment of roles and responsibilities. ECD: April 30, 2021.

**OIG Analysis of CBP Comments:** CBP's proposed action is responsive to the recommendation. However, if maintaining separate testing groups, the intent of our recommendation also is to ensure stronger coordination between the groups. We consider this recommendation resolved and open. It will remain open until CBP presents the results of the Deputy Commissioner's decision and associated delegations of roles and responsibilities.

**CBP Comments to Recommendation 3:** Concur. Operations Support, in collaboration with OI and Border Patrol, will form a working group to study the effectiveness of maintaining multiple covert testing groups within CBP and present results to the Deputy Commissioner. The presentation will include proposed assignment of roles and responsibilities. ECD: April 30, 2021.

**OIG Analysis of CBP Comments:** CBP's proposed action is responsive to the recommendation. We consider this recommendation resolved and open. It will remain open until CBP provides its new standard operating procedures.

**CBP Comments to Recommendation 4:** Concur. Operations Support and OI leadership teams will develop a proposal for the Deputy Commissioner's consideration to determine the best placement of OFTD within CBP's and OFTD's authority. ECD: April 30, 2021.

**OIG Analysis of CBP Comments:** CBP's proposed action is responsive to the recommendation. We consider this recommendation resolved and open. It will remain open until CBP provides documentation on the results of its determination and delegation of OFTD's authority.

**CBP Comments to Recommendation 5:** Concur. CBP described the processes OFTD and Border Patrol currently use for data collection, data monitoring, and supervisory review. Additionally, OFTD and Border Patrol will develop performance measures to assess the effectiveness of their covert testing programs. OFTD will also develop standard operating procedures. ECD: April 30, 2021.

**OIG Analysis of CBP Comments:** CBP's proposed actions are responsive to the recommendation. We consider this recommendation resolved and open. It will remain open until CBP provides documentation of OFTD and Border Patrol processes and procedures for data collection, monitoring, supervisory review, and performance measures developed for the covert testing programs.

**CBP Comments to Recommendation 6:** Concur. OFTD is developing a new database to collect covert test results and provide various reporting functionalities. Starting October 1, 2019, Border Patrol required all units to input assessments into its centralized database. ECD: April 31, 2021.

**OIG Analysis of CBP Comments:** The actions described by OFTD and Border Patrol are responsive to the recommendation. We consider this recommendation resolved and open. It will remain open until the two testing groups fully implement all facets of their databases and provide the OIG a demonstration of their functionality and examples of the types of outputs or reports they produce.

**CBP Comments to Recommendation 7:** Concur. CBP's Office of Personnel Responsibility completed its review of classified reports and provided its results to the OIG on May 7, 2019. Additionally, CBP provided documentation that all OFTD staff attended derivative classification training for the proper identification, marking, and handling of classified information. CBP requested closure of the recommendation.

**OIG Analysis of CBP Comments:** CBP's actions are partially responsive to the recommendation. However, we do not believe the completed actions are adequate to close the recommendation. CBP has not provided the OIG with copies of declassification instructions it issued to offices receiving the reports that prompted our classification challenge. Additionally, CBP did not address how OFTD is re-marking its documents that OPR determined were over-

marked. This recommendation will remain open and unresolved until CBP provides additional information on how OFTD will address and provide instructions for declassifying over-marked documents.

## Appendix A
## Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine whether CBP's covert testing is identifying vulnerabilities at ports of entry and borders and whether CBP uses the test results to address identified vulnerabilities and share lessons learned throughout the component. To answer our objective, we:

- researched laws, regulations, and policies to identify applicable criteria pertaining to CBP's covert testing requirements;
- obtained and reviewed priorities and strategic plans including OFO and Border Patrol priorities for FY 2016 to FY 2018, Office of Intelligence priorities for FY 2017 to FY 2018, and OFO's strategic plans for FY 2016 to FY 2018;
- analyzed SOPs established between OFTD and program offices within CBP; and
- analyzed draft directives and letters describing the authorities of OFTD and CPMO.

We also assessed OFTD's covert testing budgets from FY 2016 through FY 2018 and requested information about its performance metrics to assess how OFTD planned its covert testing. We reviewed and analyzed:

- 85 classified and unclassified OFTD test results from FY 2014 to FY 2018, and
- classified OFTD and DHS Countering Weapons of Mass Destruction (formerly Domestic Nuclear Detection Office) test results from FY 2014 to FY 2018.

To analyze CBP's covert test reporting process, we reviewed report transmission emails and covert testing notification emails. We analyzed a sample of tests to assess whether operations plans indicated how often follow-up testing occurred or whether test reports made recommendations to address non-interdictions. We also reviewed CIAP test reports that CPMO was able to gather from October 2014 through June 2018 and reviewed sector covert testing SOPs.

We requested and reviewed corrective action plans to determine whether CBP documented resolution of actions taken. We assessed the reliability of OFTD's covert testing database by reviewing operation plans and covert testing

summary reports in combination with OFTD's covert testing FY 2018 budget for all smuggling campaign tests, which took place from May to August 2018.

We conducted a site visit to [redacted] International Airport to observe covert test planning, execution, and the debriefing process. We also interviewed port officials in the Chicago Field Office following an express consignment covert test.

We interviewed officials from:

- Office of Intelligence Analysis Directorate
- Office of Intelligence executive leadership
- Operational Field Testing Division
- Office of Field Operations
- Border Patrol
- Countering Weapons of Mass Destruction (formerly Domestic Nuclear Detection Office)
- OIG Office of Audits subject matter experts in TSA covert testing
- TSA Office of Inspections
- CBP executive leadership

We conducted this performance audit between June 2018 and August 2019 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.

# Appendix B
# CBP Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

May 15, 2020

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Henry A. Moak, Jr.
Senior Component Accountable Official
U.S. Customs and Border Protection

SUBJECT: Management Response to Draft Report: "CBP Needs a Comprehensive Process for Conducting Covert Testing and Resolving Vulnerabilities" (Project No. 18-098-AUD-CBP)

Thank you for the opportunity to 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.

CBP is pleased that the OIG recognized the importance of, and contributions made by, CBP's Operational Field Testing Division (OFTD) and Checkpoint Internal Assessment Program (CIAP) to CBP's mission to safeguard U.S. borders by preventing illegal movement of people and contraband through land, sea, and air ports of entry, as well as between ports of entry and at interior checkpoints. To safeguard U.S. borders, CBP uses a multi-layered enforcement strategy, which incorporates a variety of tools and techniques. CBP established OFTD and CIAP to conduct covert testing to evaluate the effectiveness of the Office of Field Operations (OFO) and U.S. Border Patrol's (USBP) implementation of this strategy.

CBP is concerned, however, that OIG's draft report contains several inaccurate and misleading representations, including the definition of "risk" OIG applies to CBP testing methodologies. All this is despite OIG's numerous meetings with CBP's program officials, subject matter experts, and others; and CBP's sharing of extensive supporting documentation with OIG since OIG announced this audit on June 21, 2018, ***nearly two years ago***. For example, the report references "risk" numerous times throughout and states simply that CBP covert testing teams do not utilize risk assessments, and accordingly do not comply with the Trade Facilitation and Trade Enforcement Act (TFTEA) (which requires "risk-based" testing). This conclusion could only be reached

by OIG still fundamentally misunderstanding Homeland Security risk management doctrine and CBP's covert testing program.

The OIG implies that covert testing should be driven by risk assessments. This is the inverse of the CBP covert testing approach. CBP's covert testing activities are driven by senior managers' requests to identify *unknown risk versus known risk*. The findings from these assessments inform CBP's risk management strategies. The risk-based approach identifies the highest *compliance* risks to the organization and makes them the priority for controls, policies, and procedures.

Risk identification is a part of the overall risk management and assessment process. *DHS Risk Management Fundamentals* (April 2011) discusses the need for maintaining "good situational awareness" as part of the risk management effort. Monitoring such good situational awareness is "essential if risk management efforts are to be effective over time." The guide discusses models of evaluation: "[R]ed teaming (scenario role-playing), exercises, external review, and surveys. Different models of evaluation will require differing levels of involvement from organization leadership and staff. For example, red teaming and exercises should be guided by leadership and analysts." Operational risks include those that impact personnel, time, materials, equipment, tactics, techniques, information, technology, and procedures that enable an organization to achieve its mission objectives. This aligns with the *DHS Risk Management Fundamentals*, which explain that "Prior to conducting a risk assessment, it is valuable to make a concerted effort to identify risks beyond those usually considered. For example, risks that are newly developing, even if they are poorly understood, are useful to identify. Risks that are highly unlikely but have high consequences should also be identified and incorporated into the assessment, if possible. This can even include identifying the risk of the unknown as a possible risk."

The OIG recognizes that covert testing assessments are driven by senior CBP leadership's direction to focus them on identifying unknown operational risk and readiness. Covert testing is designed to identify whether strengths, weaknesses, or vulnerabilities confirm or confute leadership's assumptions and will lead to enhanced probability of detection of illicit contraband and travelers. OFTD and USBP testing methodologies follow well-established red teaming doctrine developed by the Department of Defense and adopted by other red teams within DHS and across the federal government, such as the 1st Information Operations Command and the Defense Threat Reduction Agency. CBP's red team techniques for identifying risk follow the *DHS Risk Management Fundamentals*, *e.g.*, "Brainstorming is a common technique to identify these unusual, emerging, and rare risks. So, too, is involving a wide range of perspectives and strategic thinkers to avoid the trap of conventional wisdom and groupthink."

2

The draft report also states that CBP does not comprehensively plan and conduct its covert testing and use its test results to address vulnerability. That is false. OFTD, with OFO and USBP, does in fact perform these activities. OFTD proposed, planned, and conducted four major system-wide campaigns with OFO and USBP during Fiscal Year (FY) 2019. These campaigns crossed several field offices and sectors, and the findings resulted in operational office leadership: (1) issuing musters; (2) making changes to standard operating procedures (SOPs); and (3) implementing technology upgrades. OIG does not mention this in its draft report.

CBP covert testing teams do not measure operational success by detection or interdiction. OIG's draft report bases its conclusions on quantitative measures in the form of recommendations due to specific interdiction results, but does not account for the qualitative values and purpose that drive a specific testing campaign. Such testing is not based on interdiction results; rather, the purpose is to acquire a better situational awareness of current processes that exist throughout the operational environment often resulting in a non-interdiction with no action being required.

In addition, OIG's draft report misconstrues in several ways the assessment that that audit team observed. For example, the draft report states that OFTD did not report non-interdictions during the assessment to CBP officials for awareness and corrective action. However, CBP reported all results in alignment with the agreed upon objectives with the program office and codified in the operations plan. Further, because senior CBP officials were involved in the assessment as it occurred, subsequent reporting of non-interdictions was unnecessary; however, OIG staff witnessed the Port Director issue new local SOPs to address the identified risks vulnerabilities.

OIG says that CBP does not conduct system-wide testing prior to gathering intelligence to determine risk or priority level or coordinate with USBP. OIG cites in support the series of assessments conducted by OFTD in concert with USBP, throughout multiple sectors. This is not only highly inaccurate but contradicts OIG's previous statements. Indeed, this system-wide testing was done in collaboration with the Checkpoint Programs Management Office (CPMO) and USBP sector personnel. Testing was based on previous testing results in multiple sectors, and in response to a study conducted by University of Arizona (that DHS commissioned) that found "that the best indicator of checkpoint performance is to measure the accuracy rate of the Border Patrol in detecting illegal activity, such as false documents, illicit drugs, and nuclear radiation. The most feasible and reliable method for calculating these accuracy rates is through 'red teaming.'"

Further, OIG's draft report claims that OFTD did not provide these test results to the Office of Intelligence (OI) to inform their intelligence products. Again, that is false. In fact, OFTD shared all test results with OI in multiple ways (email and weekly senior staff

meetings). OIG also claims that OFTD and USBP do not coordinate. But all OFTD testing is coordinated through the CPMO, which includes both OFTD and USBP representation. OIG compounds its error by saying that "to enhance coordination, Border Patrol provided detailees to OFTD, but this has not happened consistently." However, since FY 2018, every USBP sector assessment has predominantly consisted of USBP personnel, to include their serving as team leads.

CBP previously submitted written technical comments under a separate cover for OIG's consideration. These comments highlighted several factual and contextual concerns. To OIG's credit, the team conducting this audit provided some feedback on how OIG planned to adjudicate these comments. However, it is not clear whether the concerns were adequately addressed because the team was unwilling to share a revised copy of its draft report with CBP prior to final report publication.

The draft report contained seven recommendations, with which CBP concurs. CBP agrees that effective covert testing is an essential part of a multi-layered strategy to effectively guard against dangerous people and materials that threaten the nation's security and remains committed to continuously improving its covert testing programs. Attached find our detailed response to each recommendation.

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.

Attachment

**Attachment: Management Response to Recommendations Contained in 18-098-AUD-CBP**

OIG recommended that the Deputy Commissioner of CBP:

**Recommendation 1:** Develop and implement policies to ensure CBP's covert testing groups:

a. develop risk-based annual covert test plans and identify systemic tests;
b. distribute test results throughout the organization;
c. make recommendations; and
d. implement and track corrective actions.

**Response:** Concur. Once CBP Operations Support (OS), in collaboration with the Offices of Intelligence (OI), and U.S. Border Patrol (USBP) determine the effectiveness of maintaining multiple covert testing groups and placement of covert testing, CBP will develop standard operating procedures and policies for risk-based covert testing, as appropriate. Estimated Completion Date (ECD): April 30, 2021.

**Recommendation 2:** Study the effectiveness of maintaining multiple covert testing groups, and if CBP maintains multiple groups, we recommend specifying roles, responsibilities, and requirements for coordination to eliminate redundancies.

**Response:** Concur. CBP OS, in collaboration with OI and USBP will form a working group to study the effectiveness of maintaining multiple covert testing groups. This group will provide the Deputy Commissioner with an analysis for consideration, to include the proposed assignment of roles and responsibilities for planning and conducting covert tests, making recommendations, and overseeing corrective actions. ECD: April 30, 2021.

**Recommendation 3:** Assign roles and responsibilities for:

a. planning and conducting covert tests;
b. making recommendations; and
c. overseeing corrective actions through resolution.

**Response:** Concur. Within CBP, the Policy Directorate is functionally responsible for the development and implementation of enterprise-wide policy, directives and binding memorandums, however, it does not have operational functions responsible for managing field deployable assets. Consequently, CBP OS, in collaboration with OI and USBP will form a working group to study the effectiveness of maintaining multiple covert testing

groups. This group will provide the Deputy Commissioner with an analysis for consideration, which will include the proposed assignment of roles and responsibilities for planning and conducting covert test, making recommendations, and overseeing corrective actions. ECD: April 30, 2021.

**Recommendation 4:**

a. assess organizational placement and resources of Operational Field Testing Division to determine the best placement in CBP's organizational chart, and
b. provide OFTD authority to plan and conduct independent, system-wide tests, make recommendations, and track corrective actions.

**Response:** Concur. The CBP OS and OI leadership teams will develop a proposal for the Deputy Commissioner's consideration to determine the best placement of the OFTD within CBP, and OFTD's authority. ECD: April 30, 2021.

OIG recommended that the Assistant Commissioner Office of Intelligence and Border Patrol's Chief of Law Enforcement Operations Directorate:

**Recommendation 5:** Direct covert testing entities to develop and implement both performance measures and standard operating procedures including:

a. processes for determining data to be included in test reports,
b. data quality monitoring, and
c. supervisory review.

**Response:** Concur. CBP OFTD currently has a process to determine what data is included in test reports, data quality monitoring, and supervisory review. All data collection is done in collaboration with the CBP program office and is reflected in standardized checklists. Data generated from these checklists are reviewed by the team lead before being added to a database. Prior to conducting any comprehensive data analysis, a separate reconciliation review of test data and reports is conducted by senior management in the headquarters' program office, the field office or sector, and OFTD, as appropriate, before the data is finalized. OFTD will develop performance measures and standard operating procedures to assess the effectiveness of the program in collaboration with USBP and the Office of Field Operations.

USBP currently utilizes an operational planning process for internal covert testing assessments, and CIAP units conduct assessments through local team leads with direct management oversight at both the Sector and Headquarters levels. Data collected via these assessments is systematically input into an operations planning format according to an operational planning process prior to implementation. This process requires

coordinating efforts of CIAP units to include sector planning and intelligence units, to ensure a multi-perspective approach for a more in-depth analysis of the operational environment. The process accounts for data collection, interpretation, and quality monitoring, and includes supervisory review and approval before information is disseminated to leadership for appropriate action. USBP will develop performance measures as they pertain to covert tests, as appropriate. ECD: April 30, 2021.

**Recommendation 6:** Direct covert testing entities to develop and implement databases to record test results, recommendations, and the status of corrective actions.

**Response:** Concur. In coordination with the CBP Office of Information and Technology, OFTD is currently in Phase II of database development. In the first phase, results information, and all FY 2019 and 2020 covert test planning was uploaded. For Phase II, OFTD is now revising database requirements to improve database workflow, functionality, and capabilities of the system. Phase III is on schedule to be complete in FY 2020, and will incorporate: system and flag generated email notifications, dashboard, and report features. The corrective action portion of the database will be developed in Phase IV.

USBP utilizes a centralized database to capture CIAP assessments. Starting October 1, 2019, all CIAP units were required to begin the input of internal assessments according to existing USBP operational planning guidelines. The functionality of the database is consistent with the elements required of CIAP assessments and allows for data captures of test results via after action reports, recommendations, and any subsequent course of action. ECD: April 30, 2021.

OIG recommended that the Assistant Commissioner Office of Intelligence:

**Recommendation 7:** Direct all Operational Field Testing Division staff to review all prior and future classified reports to ensure they are properly marked to protect national security information.

**Response:** Concur. CBP's Office of Professional Responsibility (OPR) reviewed all classified reports, the results of which were communicated in a May 7, 2019, Memorandum titled "Classification Challenge Decision" from the OI Assistant Commissioner, to the OIG. This Memorandum notified the audit team of OPR review and determination of the previously classified records.

In addition, by September 2019, all OFTD staff attended OPR refresher Derivative Classification training, for the proper identification, marking and handling of classified information. Supporting documentation was previously provided to the OIG. CBP requests that the OIG consider this recommendation resolved and closed, as implemented.

7

## Appendix C
## Office of Audits Major Contributors to This Report

Christine Haynes, Audit Director
Heidi Einsweiler, Audit Manager
Loretta Atkinson, Audit Manager
Denis Foley, Analyst-in-Charge
Diane Benton, Program Analyst
Callece Gresham, Program Analyst
Jane DeMarines, Communications Analyst
Junior Correa, Independent Referencer

# Appendix D
# Report Distribution

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

**U.S. Customs and Border Protection**

Acting Commissioner, Customs and Border Protection
Executive Assistant Commissioner, Office of Field Operations
Chief, U.S. Border Patrol
Assistant Commissioner, Office of Intelligence

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

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