OFFICE OF INSPECTOR GENERAL

CBP Faced Challenges in Its Inspection Processes and Physical Security at the JFK International Mail Facility (REDACTED)

Homeland Security

March 12, 2021

OIG-21-27

March 4, 2021

MEMORANDUM TO: Troy Miller
Senior Official Performing the
Duties of the Commissioner
U.S. Customs and Border Protection

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

JOSEPH V CUFFARI

Digitally signed by JOSEPH V CUFFARI
Date: 2021.03.04 13:58:49 -05'00'

SUBJECT: *CBP Faced Challenges in Its Inspection Processes and Physical Security at the JFK International Mail Facility –* ~~*For Official Use Only*~~

Attached for your information is our final report, *CBP Faced Challenges in Its Inspection Processes and Physical Security at the JFK International Mail Facility–* ~~*For Official Use Only.*~~ We incorporated the formal comments from U.S. Customs and Border Protection in the final report.

The report contains eight recommendations aimed at improving international mail processes at JFK International Airport. CBP concurred with six recommendations and non-concurred with two recommendations. Based on the information provided in response to our draft report, we consider recommendations 1, 2, and 3 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) target completion date for each recommendation, and (2) corrective action plans for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendations. Please send your response to or closure request to OIGAuditsFollowup@oig.dhs.gov.

Based on information provided in your response to the draft report, we consider recommendations 4, 5, 6, 7, and 8 open and resolved. Once your office has fully implemented these five 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.

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 Thomas Kait, Acting Assistant Inspector General for Audits, at (202) 981-6000.

Attachment

cc: Sanjeev Bhagowalia, Acting Assistant Commissioner, Office of Information and Technology
William A. Ferrara, Executive Assistant Commissioner, Office of Field Operations
Pete Flores, Acting Executive Assistant Commissioner, Operations Support

DHS OIG HIGHLIGHTS
CBP Faced Challenges in Its Inspection Processes and Physical Security at the JFK International Mail Facility

Why We Did This Audit

One of CBP's top priorities is safeguarding the public by preventing imports of opioids and other illegal items mailed from overseas through the USPS. As a follow-up to our September 2018 report, we conducted this audit to determine whether CBP's airmail, physical security, and inspection processes at the JFK International Airport are adequate to effectively screen, track, and safeguard incoming international mail.

What We Recommend

We made eight recommendations to CBP that addressed resources, guidance, space, controls, and security needed to prevent imports of illegal drugs and contraband through the JFK IMF.

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's (CBP) mail inspection processes and physical security at the John F. Kennedy (JFK) International Mail Facility (IMF) have not improved since our prior audit. CBP only inspected approximately ■ percent of the 1.3 million pieces of mail it received during our June 2019 site visit. CBP also did not timely inspect and process mail from high-risk countries, creating unmanageable backlogs. These deficiencies were largely due to inadequate resources and guidance. Consequently, more than ■■■■ pieces of mail were sent out for delivery without physical inspection.

Successful execution of CBP's targeting and interdiction of prohibited items was hindered, as CBP could not fully account for the targeted mail provided by United States Postal Service (USPS). CBP's targeting of mail for potential violations also had a ■ percent detection rate due to inconsistent and incomplete advanced data on mail content. Amid these challenges, CBP could not ensure that targeted mail was inspected before delivery.

Further, physical security controls, such as locks and cameras, were not adequate to fully safeguard mail in CBP's possession. Deficient physical security controls can lead to unauthorized access to restricted areas, misplacement of prohibited items, or exposure to dangerous substances.

Lastly, controls over the information technology infrastructure and systems supporting mail processing were not fully effective. CBP did not correctly patch a server or ensure system controls of a database containing targeting information. CBP also had not conducted a Privacy Threshold Analysis on a local database at JFK, placing personal data stored in the system at risk.

Management Response

CBP concurred with recommendations 2, 4, 5, 6, 7, and 8, but did not concur with recommendations 1 and 3.

Table of Contents

Appendixes

Abbreviations

ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CCTV	closed-circuit television
C.F.R.	Code of Federal Regulations
COI	Countries of Interest
GAO	Government Accountability Office
IMF	International Mail Facility
IT	information technology
JFK	John F. Kennedy International Airport
MOU	Memorandum of Understanding
TSA	Transportation Security Administration
U.S.C.	United States Code
USPS	United States Postal Service

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Background

U.S. Customs and Border Protection's (CBP) mission includes preventing contraband, including illegal drugs and terrorist weapons from entering the United States, while also facilitating the flow of legitimate international travel and trade. CBP plays a critical role in interdicting illegal drugs and other contraband at mail facilities. Imports of opioids such as fentanyl, are a serious problem. In 2018, more people in the United States died from opioid-related causes than from traffic accidents. According to a 2019 report[1] by the Council of the Inspectors General on Integrity and Efficiency, opioids are often produced by drug traffickers overseas and illegally trafficked into the United States across its border or through mail or parcel delivery services. Airports are known to be major entry points for illegal drug imports. Given its frontline responsibility to secure the Nation from imports of illegal drugs and contraband, CBP has a major role to play in helping end the opioid crisis.

To prevent illegal substances from entering the country, all inbound international airmail is subject to CBP inspection, except for mail known or believed to contain only official documents addressed to U.S. Government officials or ambassadors of foreign countries.[2] In addition to collecting duties on imported merchandise, CBP is required to examine mail for contraband or other illegally imported articles, including restricted or prohibited merchandise.[3] Additionally, CBP is responsible for inspecting agricultural products mailed from foreign countries to the United States.[4]

CBP is not the only participant in the international airmail inspection process. For example, the Transportation Security Administration (TSA) initially requires that foreign airports and air carriers screen international cargo headed to the United States. TSA also inspects air carrier operations at international locations to ensure compliance with security program requirements. The United States Postal Service (USPS) is another key partner in the inspection of international mail. CBP and USPS have established a memorandum of understanding (MOU) on guidelines for working together nationwide to process

---

[1] *Combatting the Opioid Crisis: Role of the Inspector General Community,* Council of the Inspectors General on Integrity and Efficiency, September 2019.

[2] According to the *Memorandum of Understanding between CBP and USPS Regarding Cooperation in the Inspection of Goods Imported or Exported through the Post,* September 1, 2017 CBP has responsibility for inspection and clearance of all international mail arriving from foreign origins and overseas military post offices, intended for delivery into the Customs territory of the United States and U.S. Virgin Islands. Also, *see* 19 Code of Federal Regulations (C.F.R) § 145.2(b).
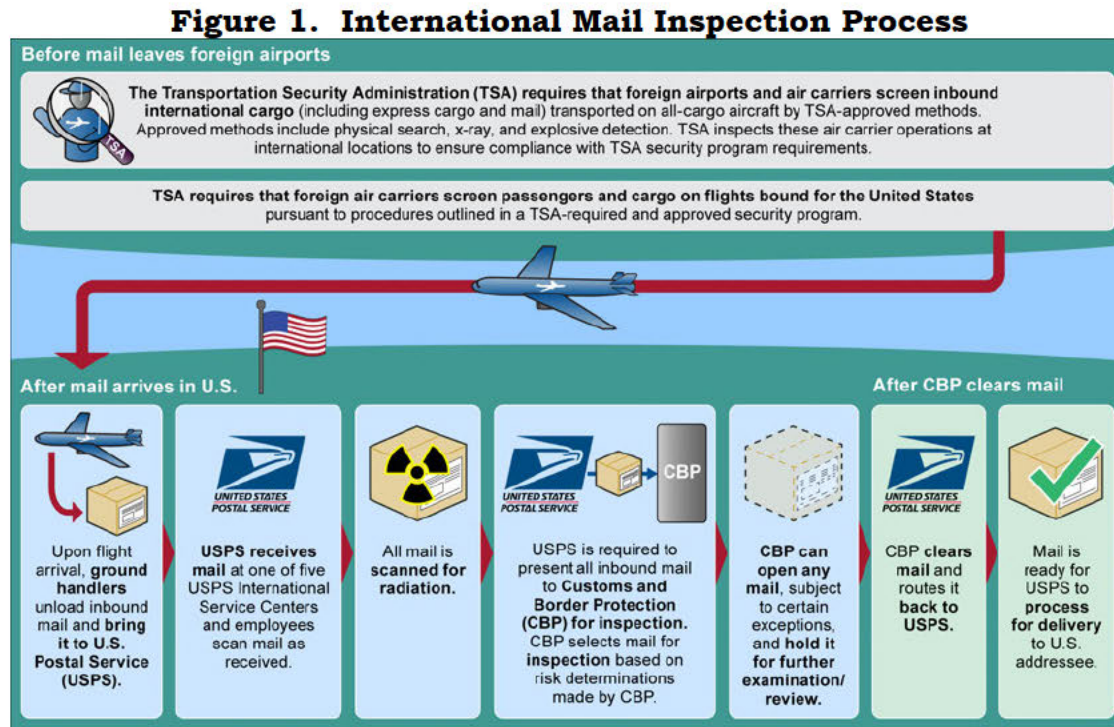
[3] *Ibid.*

[4] 19 C.F.R., "Customs Duties," and Public Law, 107-296, *Homeland Security Act of 2002.*

arriving international air mail.[5] Figure 1 shows the basic flow of incoming mail as the cargo is screened by TSA, received by USPS, and presented to CBP for inspection and clearance before delivery to U.S. addresses.

Figure 1. International Mail Inspection Process

Before mail leaves foreign airports

The Transportation Security Administration (TSA) requires that foreign airports and air carriers screen inbound **international cargo** (including express cargo and mail) transported on all-cargo aircraft by TSA-approved methods. Approved methods include physical search, x-ray, and explosive detection. TSA inspects these air carrier operations at international locations to ensure compliance with TSA security program requirements.

TSA requires that foreign air carriers screen passengers and cargo on flights bound for the United States pursuant to procedures outlined in a TSA-required and approved security program.

After mail arrives in U.S.

After CBP clears mail

| Upon flight arrival, **ground handlers** unload inbound mail and **bring it to U.S. Postal Service (USPS).** | **USPS receives mail** at one of five USPS International Service Centers and employees scan mail as received. | All mail is **scanned for radiation.** | USPS is required to present all inbound mail to **Customs and Border Protection (CBP)** for inspection. CBP selects mail for inspection based on risk determinations made by CBP. | **CBP can open any mail,** subject to certain exceptions, and **hold it for further examination/ review.** | **CBP clears mail** and routes it **back to USPS.** | Mail is ready for USPS to **process** for delivery to U.S. addressee. |

Source: Government Accountability Office (GAO), *Costs and Benefits of Using Electronic Data to Screen Mail Need to Be Assessed,* GAO-17-606, August 2, 2017[6]

CBP's Airmail Inspection Process at the JFK International Mail Facility

The USPS International Service Center at John F. Kennedy International Airport (JFK) is the largest of nine USPS facilities nationwide that receive and process incoming international mail. This location is the gateway into the United States for approximately 60 percent of all international mail, which includes First Class Mail, Registered Mail, Express Mail, and Priority Parcels. In fiscal year 2019, USPS recorded an inbound international mail volume at JFK of nearly 205 million pieces of mail — nearly 560,000 pieces per day. This constitutes approximately 44 percent of the hundreds of millions of pieces of

---

[5] *Memorandum of Understanding between CBP and USPS Regarding Cooperation in the Inspection of Goods Imported or Exported through the Post,* September 1, 2017.
[6] In the GAO-17-606 report, GAO identified nine International Service Center facilities but GAO only focused on the five International Service Center facilities that accepted majority of inbound international mail.

international mail arriving in FY 2019 at all international mail facilities (IMF) across the Nation.

CBP officials use detection, identification, and targeting capabilities along with advanced data, information sharing, and partnerships as part of its multi-faceted approach to determine what portion of the mail to select for further inspection. More specifically, CBP has a three-tiered approach for scanning and inspecting international airmail at the JFK IMF, including: (1) intelligence gathering for advanced mail targeting, (2) x-ray machine inspection and canine inspection, and (3) CBP's physical inspection and testing of mail contents. Each step is further described below.
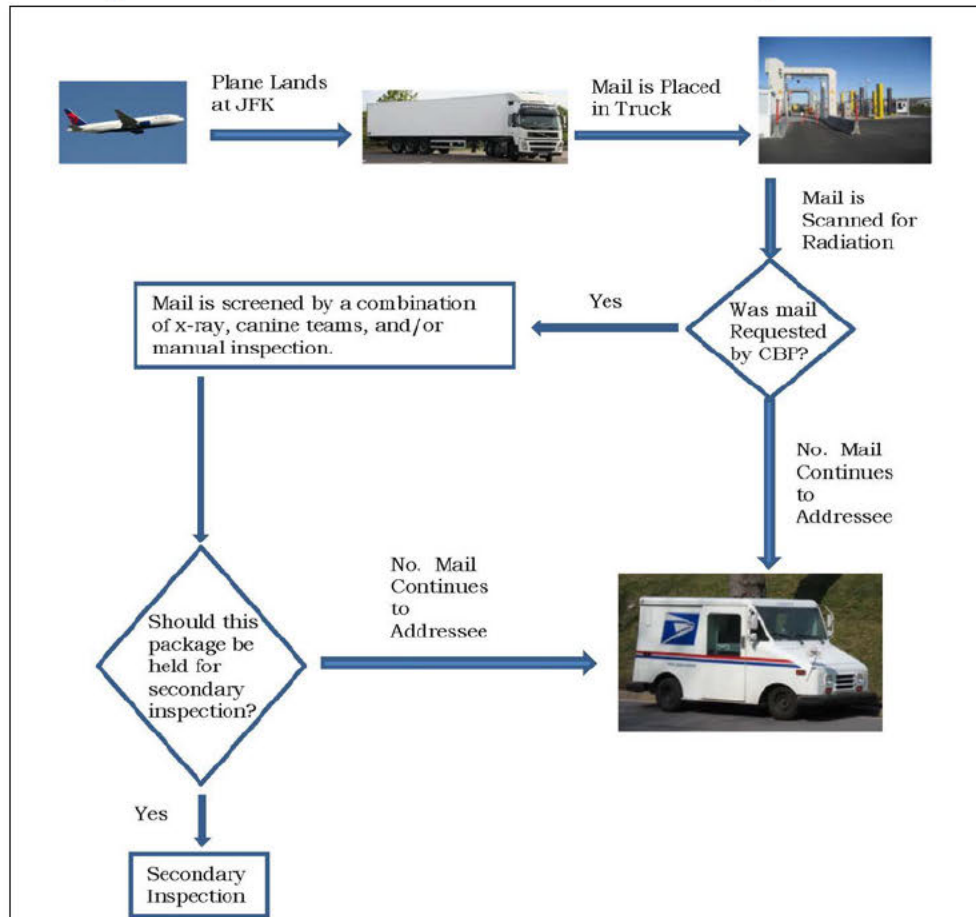
1) Advanced electronic data gathering enables CBP to target individual pieces of mail prior to arrival at JFK airport. CBP officials use a risk-based approach, as well as past experience, to identify certain mail and packages for inspection. For example, CBP uses its Automated Targeting System (ATS), a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments, to identify mail more likely to contain narcotics or other contraband.

2) CBP utilizes x-ray machines and canine teams to conduct secondary inspections to further determine whether a package should be seized or returned to USPS for processing. If, during CBP's examination, a mail item is found to contain prohibited material, such as illegal drugs, the mail package is held for further examination by CBP staff.

3) With limited exceptions, CBP can open mail packages by hand to inspect, or test, its contents. If no anomalies are found, the items are returned to USPS for delivery without further examination by CBP.

Figure 2 depicts the end-to-end flow of international airmail processing upon arrival at JFK.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 2. International Airmail Processing at JFK

Plane Lands at JFK → Mail is Placed in Truck →

Mail is Scanned for Radiation

Was mail Requested by CBP?

Yes → Mail is screened by a combination of x-ray, canine teams, and/or manual inspection.

No. Mail Continues to Addressee

Should this package be held for secondary inspection?

No. Mail Continues to Addressee →

Yes → Secondary Inspection

Source: Office of Inspector General (OIG)-developed, based on analysis of CBP-provided information

As depicted in the top right corner of Figure 2, once flights land at JFK airport, ground handlers transport the mail to USPS. All arriving international airmail is scanned through a radiation portal monitor[7] at the JFK IMF before being provided to USPS. USPS receives all incoming mail, but only provides mail to CBP for physical inspection upon CBP's request. CBP routinely requests that USPS provide broad categories of mail from specific countries, as well as targeted individual pieces of mail and mail flagged for inspection by canine teams. Arriving international airmail not requested by CBP is not physically inspected by CBP prior to delivery, as shown in the bottom right corner of Figure 2.

---

[7] The radiation portal monitor provides a passive, non-intrusive means to screen cars, trucks and other conveyances for the presence of radioactive and nuclear materials.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Previous Audit of CBP's International Mail Inspection Process at JFK

In 2017, we conducted an audit at JFK IMF to determine whether CBP airmail inspection processes were effective and had adequate information technology (IT) security controls. We reported[8] that CBP did not have effective processes and IT security controls to support airmail inspection operations at JFK. Specifically, despite legislative requirements to systematically target and prevent illegal imports, CBP physically inspected a limited number of the hundreds of thousands of pieces of incoming airmail each day, largely due to difficulty inventorying and locating targeted mail, as well as inadequate guidance, equipment, and resources. We disclosed that international mail suspected of containing contraband was not physically controlled due to procedural, space, and technical limitations. We also reported that servers supporting CBP's mail inspection processes did not meet IT security control requirements, and not all of the servers were included in CBP's system inventory. We recommended the CBP Office of Information Technology and CBP Office of Field Operations and Operations Support provide the resources, guidance, space, controls, oversight, and IT security needed to prevent imports of illegal drugs and goods.

As a follow-up to our 2017 audit, the objective of this audit was to determine whether CBP's airmail, physical security, and inspection processes at JFK International Airport IMF are adequate to effectively screen, track, and safeguard incoming international mail.

Results of Audit

CBP's mail inspection processes and physical security at the JFK IMF have not improved since our prior audit. CBP only inspected approximately ▮ percent of the 1.3 million pieces of mail it received during our June 2019 site visit. CBP also did not timely inspect and process mail from high-risk countries, creating unmanageable backlogs. These deficiencies were largely due to inadequate resources and guidance. Consequently, more than ▮▮▮▮ pieces of mail were sent out for delivery without physical inspection.

Successful execution of CBP's targeting and interdiction of prohibited items was hindered, as CBP could not fully account for the targeted mail provided by USPS. CBP's targeting of mail for potential violations also had a ▮ percent detection rate due to inconsistent and incomplete advanced data on mail content. Amid these challenges, CBP could not ensure that targeted mail was inspected before delivery.

---

[8] *CBP's International Mail Inspection Processes Need Improvement at JFK International Airport*, OIG-18-83, September 24, 2018.

Further, physical security controls, such as locks and cameras, were not adequate to fully safeguard mail in CBP's possession. Deficient physical security controls can lead to unauthorized access to restricted areas, misplacement of prohibited items, or exposure to dangerous substances.

Lastly, controls over the IT infrastructure and systems supporting mail processing were not fully effective. CBP did not correctly patch a server or ensure system controls of a database containing targeting information. CBP also had not conducted a Privacy Threshold Analysis on a local database at JFK, placing personal data stored in the system at risk.

CBP Inspects a Selected Portion of International Airmail at JFK

CBP physically inspects only a portion of the incoming international mail received at the JFK IMF daily. Additionally, CBP does not timely inspect and process targeted mail or mail from high-risk countries, creating unmanageable backlogs. CBP's physical mail inspection and processing challenges were attributed to inadequate resources and outdated guidance. More than ▮ ▮▮▮▮ pieces of international mail were sent out for delivery during our 4-day site visit without inspection, increasing the risk that prohibited and harmful items could be delivered to the public.

CBP Physical Inspections of High-risk International Airmail

According to CBP's 2001 *International Mail Operations and Enforcement Handbook*,[9] all mail intended for delivery to the United States and the U.S. Virgin Islands is subject to inspection. The mail requested or targeted by CBP, based on its advanced data gathering, may be inspected by x-ray machines, canine teams, and/or CBP officers. According to the agreement currently in place,[10] USPS will make every effort to present individual parcels targeted or requested to the designated Federal inspection area of JFK.

The JFK IMF received approximately 1.3 million mail pieces during our 4-day visit from June 17 to June 20, 2019. USPS scans mail through a radiation portal monitor. The mail inspection volume during this time is shown in Figure 3.

---

[9] Prior to 2003, certain tasks performed by CBP were performed by U.S. Customs Service which authored this 2001 Handbook in use at the time of our audit.

[10] *Standard Operating Procedures Between U.S. Customs and Border Protection, John F. Kennedy International Airport And The United States Postal Service, New York International Service Center, Regarding Cooperation In The Inspection of Goods Imported Or Exported Through The Post*, February 28, 2018.
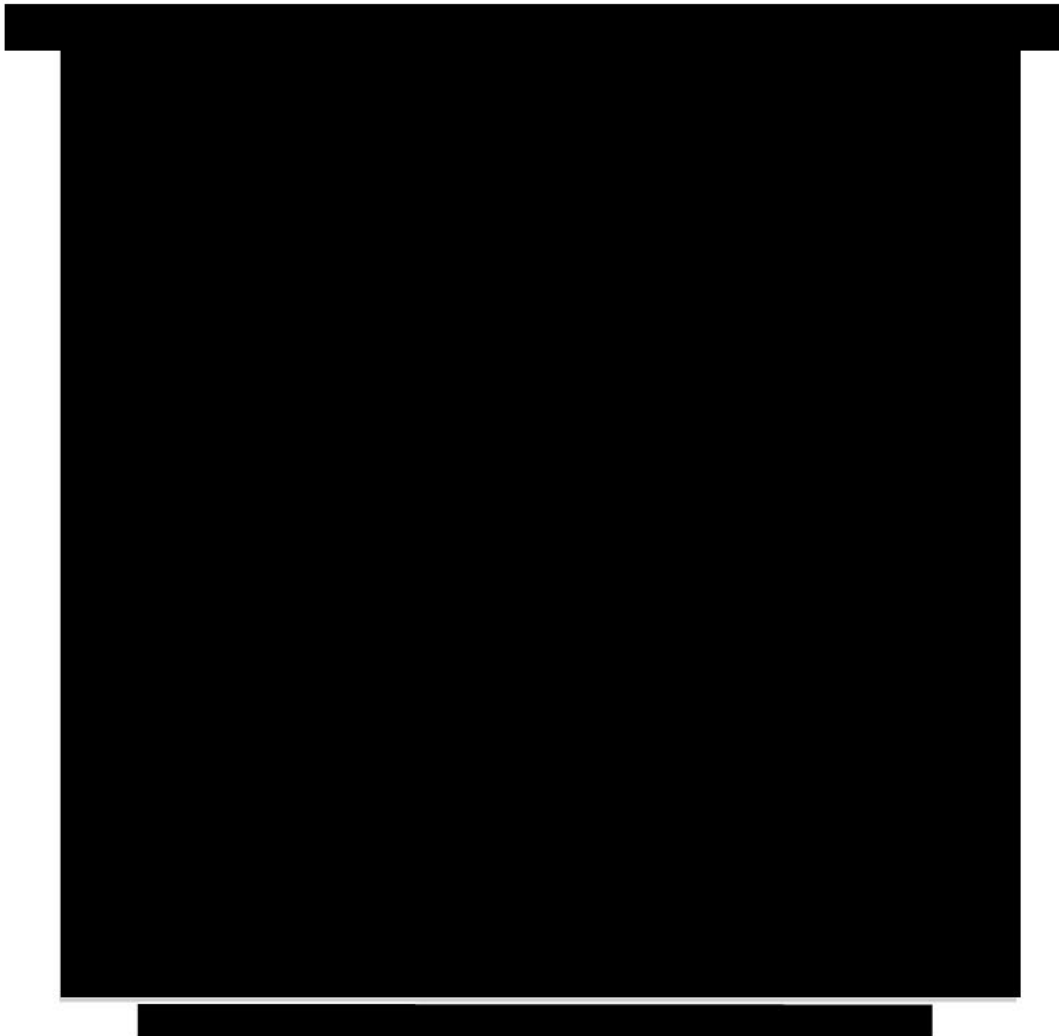
As depicted in top left corner, the JFK IMF received approximately 1.3 million mail pieces that were routed through a radiation portal monitor. Of that, CBP requested ▮▮▮▮▮▮ percent from USPS for physical inspection by x-ray machines, canine teams, and/or CBP officers, as shown on the first row of CBP processing in blue. Of the ▮▮ percent of mail requested for inspection, ▮▮ pieces were targeted by CBP using advanced electronic data. The remaining ▮▮▮▮▮ mail pieces were selected for inspection by CBP based on a number of risk factors, such as country of origin.[11] CBP returned ▮▮ percent or ▮▮▮▮▮ of the 1.3 million mail pieces to the Postal Service for delivery in the United States without physical inspection.

---

[11] CBP maintains a Countries of Interest (COI) list identifying the most likely origins of mail containing contraband.

CBP Inspected a Small Percentage of High-Risk Mail from China

Despite its responsibilities for examining mail for contraband or other illegally imported articles, CBP inspected a small percentage of high-risk mail arriving from China. CBP maintains a COI list which enables CBP officers to locate restricted items determined to most likely contain contraband. ███████████ from China is explicitly considered high-risk for containing contraband.[12] However, CBP selected less than ███████████████████ of the total targeted and ████████████ from China for inspection, as shown in Figure 4.
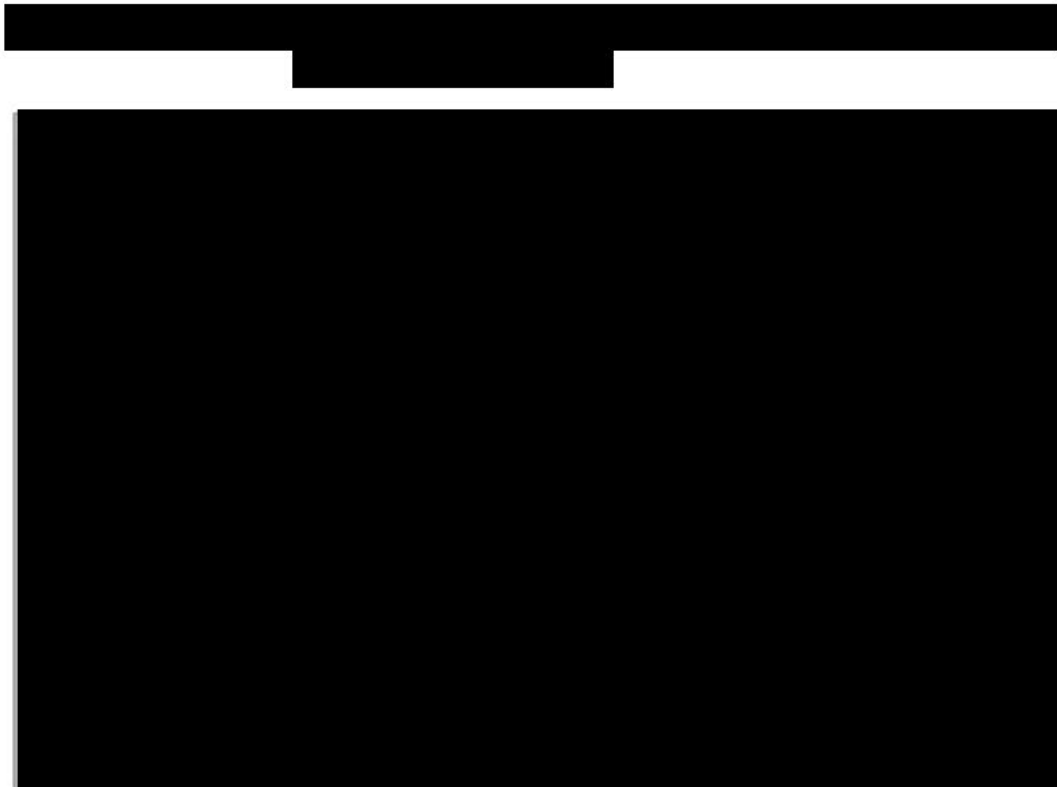
Based on USPS and CBP data, CBP received roughly 1.3 million[13] total mail pieces for all types of incoming mail between June 17 and 20, 2019.[14] Of the total 1.3 million mail pieces, 944,555 items arrived from China (including ██ targeted items and ████████████ pieces). Of ███████████████, CBP

---

[12] In January 2017, CBP conducted a 5-day blitz, Operation 'Mail Flex,' to verify that USPS was being used to mail opioids to the United States. ████████████████████████████
████████████████████

[13] 1,321,879 exact mail pieces.

[14] This represents the volume of mail requested during our June 17 – 20, 2019 onsite visit.

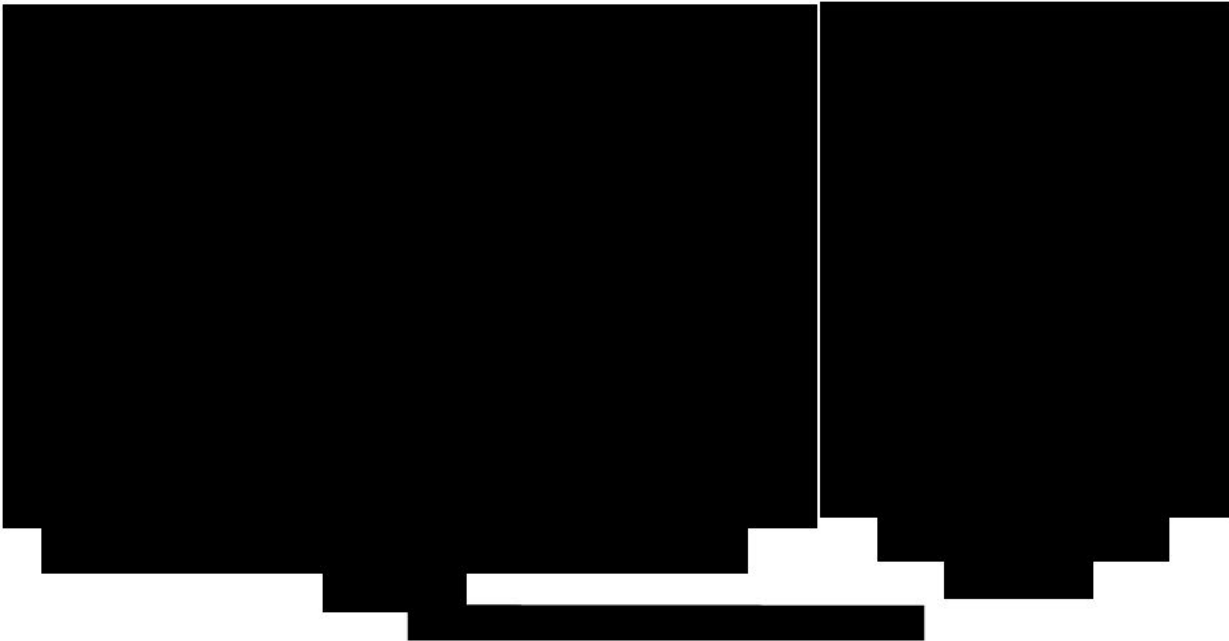requested ███████████████ for inspection, leaving ████████████████
uninspected.[15]

In addition, CBP does not fully inspect mail that is in the form of ███████
Based on our analysis of the ████████ pieces of uninspected mail from China,
███████████████████ were ████████. Figures 5 and 6 depict the total volume
of ███████ that arrived on one day during our June 2019 site visit at the JFK
IMF, waiting to be processed.

<u>CBP Did Not Conduct Accurate or Timely Inspection and Processing of High-risk Airmail</u>

CBP could not keep pace with the large volume of targeted mail from high-risk
countries arriving at the JFK IMF during our 4-day visit. CBP provides USPS
with its COI list of all classes of mail to select for inspection and processing.
The targeted parcels are placed in all-purpose containers and delivered to the
designated Federal Inspection Services area for inspection and processing. To
illustrate the ongoing volume of incoming parcels, in FY 2018, CBP received at
the JFK IMF 365 million parcels from countries on the COI list, or roughly 1

---

[15] Uninspected mail consisted of first-class mail ███████████ registered mail, and priority
parcels not targeted using advanced electronic data.

██████████████████████████████████████

million per day.[17] Of this amount, CBP estimates that it inspected, on average, ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ of mail each day. During our visit, we observed backlogs of mail at two key checkpoints: mail inspection and mail processing.

Inspection of Targeted Mail

CBP could not confirm it inspected all targeted mail from high-risk countries (i.e., mail from countries on COI list.) We reviewed CBP's ATS database at the JFK IMF to determine the exact volume of mail that was targeted from October 1, 2018 to June 30, 2019, and the time it took CBP to complete inspections. The system targeted ▮▮▮▮ percent or ▮▮▮▮▮▮▮▮▮▮ total incoming parcels. However, CBP was unable to verify the number of mail pieces it received from high-risk countries or if it had inspected all of the targeted mail.

We also noted during our visit that CBP had a backlog of targeted mail not yet inspected. According to the ATS database, it took CBP an average of 14 days after arrival to inspect the parcels. Figure 7 shows the mail inspection checkpoint, which had mail in postal containers that was more than 1 week old, but had not been inspected by CBP. The containers included mail from the COI list as well as targeted mail. USPS had provided the mail to CBP for inspection 13 days earlier.[18]

Figure 7. Backlog of Mail for Inspection
Source: OIG photo taken in June 2019

---

[17] CBP estimates of the number of COI mail parcels arriving at the JFK IMF is based on data provided by USPS. The USPS data is based on the total weight of mail provided by air carriers.

[18] The only agreement in place is the MOU between CBP and USPS, which does not specify the timeframe.

Processing of Detained and Seized Mail

CBP experienced a backlog in processing the mail it had detained during inspections. After mail pieces are inspected, CBP personnel must enter mailing information from each parcel label and USPS tracking receipt in a local database at JFK, referred to internally as the Unclaimed/Abandonment database. The information is used to apprise recipients by mail that a shipment is prohibited from entering the country. However, we noted during our visit that CBP experienced delays in entering and processing interdicted mail into the Unclaimed/Abandonment database. Figure 8 shows multiple tubs containing hundreds of packages with potentially prohibited items remained unprocessed by CBP.

Seizures are intended to keep inadmissible property out of commerce. CBP's *International Mail Operations and Enforcement Handbook*[19] states when contraband is detected and identified from a mail shipment, it must be kept in the seized property area and documented in SEACATS[20] within 24 hours. The seized contraband would be documented on a Search/Arrest/Seizure (S/A/S) Report and CF 6051, (Custody Receipt for Retained or Seized Property). CBP's *Seized Asset Management and Enforcement Procedures Handbook* [21] also

---

[19] *International Mail Operations and Enforcement Handbook CIS HB 3200-06A*, August 2001
[20] Not an acronym.
[21] *Seized Asset Management and Enforcement Procedures Handbook, HB 4400-01B*, July 2011.

requires the seizure of controlled substances to be documented on Form 6051S, (Custody Receipt for Seized Property and Evidence) in SEACATS within 24 hours after the seizure is made.

We found that CBP had a backlog of piles of Forms 6051S that had not yet been entered into SEACATS. CBP asserted it manually alerts another Government agency to inquire whether it wants to collect seized items. However, the backlog of Forms 6051S could cause further delays in timely entry and processing in SEACATS, as required by CBP's handbooks.

Inadequate Resources and Outdated Guidance Hindered CBP's Ability to Adequately Inspect and Process International Airmail

CBP's mail inspection and processing deficiencies could be attributed to inadequate resources and outdated guidance. Primarily, CBP had inadequate staffing and equipment at the JFK IMF. In addition, the canine teams are not dedicated to the JFK IMF. Lastly, CBP had not updated its *International Mail Operations and Enforcement Handbook*[22] since August 2001. Consequently, policies, procedures, and guidelines for inspecting emerging categories of mail, such as ████████, had not been instituted.

Insufficient Staff to Inspect and Process Mail at JFK IMF

CBP officials stated they did not have adequate staff to keep pace with the mail volume to inspect all targeted mail and to secure mail from sources on its COI list in a timely manner. CBP had 107 employees conducting a broad range of screening duties at the JFK IMF as of June 2019. However, CBP officials stated that this staffing level was insufficient to examine all ██████████ received each day.

Further, CBP officials said they did not have the necessary specialized staff to perform specific testing and analysis of mail. Specifically, CBP officials stated more technicians were needed to input seizure data, provide coverage after midnight, and process the high volumes of mail. The Laboratories and Scientific Services Directorate confirmed that additional personnel were necessary to perform chemical analysis and testing. As of June 2019, that Directorate had 50 chemists at its office in Newark, NJ, as asserted by CBP. CBP shared its plans to expand the Directorate staff, contingent upon obtaining additional space at the IMF in the future.

---

[22] Prior to 2003, certain CBP functions were performed by U.S. Customs Service which authored this 2001 Handbook in use at the time of our audit.

Insufficient Equipment to Conduct Mail Inspections

We determined that CBP did not have the equipment needed to inspect the hundreds of thousands of pieces of international airmail that arrive at JFK each day. For example, the JFK IMF had a total of 11 x-ray machines spread throughout the facility. Of the 11 x-ray machines, CBP only had one designated to screen ████████ However, at the time of our visit, that machine was inoperable.

CBP faced additional challenges with its equipment for conducting inspections. The existing x-ray machines were not designed to handle ██████████████ or process large volumes of mail. According to a CBP official, CBP officers did not x-ray ████████ because they jammed the x-ray machines. One CBP official informed us that an alternative for targeting ████████ was to rely on advanced electronic data processes, which had already captured prior violations, rather than screen mail from high-risk countries using x-ray machines. The alternative would enable USPS to flag a parcel upon request based on targeting information and CBP to inspect it upon arrival at the JFK IMF.

Chemical analyzers are used to identify a broad range of unknown chemicals and explosives in the field quickly and safely. Chemical analyzers can test a sample of a mailed substance without opening the package in which it came.[23] At the time of our visit in June 2019, CBP had three hand-held chemical analyzers available, but only one was used (see Figure 9). CBP staff informed us the second hand-held chemical analyzer stayed fully charged and stored as a back-up device. CBP Officials stated the third hand-held analyzer was merely on loan from a vendor.

In our prior audit report in 2018,[24] we recommended that CBP conduct an analysis to determine the additional staff, canines, x-ray scanning machines, and hand-held chemical devices needed to adequately address threats from opioids arriving daily in large volumes at the facility. During this audit, CBP provided a draft Capability Analysis Report identifying canine, staffing, and equipment gaps for the JFK IMF. In September 2020, CBP reported it had increased canines, equipment, and on-site lab staffing at JFK. CBP also reported it would receive an additional two canine teams for the JFK IMF, as well as two dedicated chemical analyzers.

CBP officials told us during this audit that many of its long-term plans were on hold because of space limitations at the JFK IMF. CBP planned to expand its resources over the coming years. However, the expansions were contingent upon obtaining extra space in the facility, which was occupied by dozens of outdated and unused chutes.[25] The chutes had not been used in approximately 9 years and had a substantial footprint at the JFK IMF. To illustrate, as of June 2019, CBP was renting a total of 64,164 square feet of space at the JFK IMF, of which the unused chutes occupied 18,000 square feet, or 28.05 percent. One row of chutes is depicted in Figure 10. Several free-standing chutes were also situated throughout the facility, blocking various mail inspection operations. Figure 11 shows a chute that was no longer in use in the agricultural area, occupying a large portion of the agriculture screening area.

---

[24] *CBP's International Mail Inspection Processes Need Improvement at JFK International Airport* (OIG-18-83), issued September 24, 2018.
[25] The term "chute" was used in conversation by CBP staff; however, the JFK IMF business plan uses the term "Conveyer System."

Figure 10. Unused Postal Chutes in the JFK IMF

Figure 11. Unused Postal Chutes

Source: OIG photos taken June 2019

In addition to the space constrictions, CBP paid rent on these unused sections of the facility that it could not access. Until the unused chutes are removed, CBP cannot implement its planned improvements at the JFK IMF.

Canine Teams are Not Dedicated to the JFK IMF

At the time of our visit, a CBP official stated the JFK IMF had 10 narcotic canine teams trained to detect fentanyl, cannabis, hashish, cocaine, and methamphetamine in mail packages. According to the CBP official, the two agricultural canines are trained to detect meat, fruit, vegetables, seeds for planting, trophies, and live animals inside of packages. However, CBP reported that none of the 12 canine teams were assigned or dedicated solely to the JFK IMF at the time. CBP officials asserted that these canine teams are an essential part of the inspection process.

Canines sniff packages on a 15-foot conveyor belt, as pictured in Figure 12, which helps in detecting controlled substances and other contraband. During our visit, we witnessed the seizure of a prohibited substance, as pictured in Figure 13, resulting from canine detection.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

| **Figure 12. Canine sniffing mail** | **Figure 13. Methamphetamine drug** |

Source: OIG photos taken June 2019

CBP Should Update Its Guidance to Capture Mail Volume and Complexity

CBP personnel do not have adequate, up-to-date guidance to manage the rapidly increasing volume and threats associated with international mail. As we reported in 2018, CBP had not updated its *International Mail Operations and Enforcement Handbook*[26] since August 2001, nearly 20 years earlier. The outdated guidance also did not contain detailed information or procedures for processing newer, designer drugs[27] such as opioids and fentanyl. Additionally, day-to-day policies, procedures, and guidelines for inspecting emerging categories of mail, such as ▮▮▮▮▮▮, had not been instituted. We previously recommended CBP update its international mail inspection handbook. During a follow up request to CBP, we were informed that the handbook is currently being updated with an estimated completion date of December 31, 2024.

Inadequate Inspection and Processing of International Airmail Increased the Risk of Mishandling or Delivering Dangerous Mail

CBP's mail inspection at the JFK IMF was inadequate to prevent illegal drugs and contraband from entering the United States. As previously stated, during our June 2019 site visit, CBP returned ▮▮▮▮▮▮▮▮▮▮▮▮▮▮ of 1.3 million international mail pieces to USPS for delivery across the nation without inspection. Without adequate inspection, prohibited and harmful items could be processed, without being tested, and delivered to the public via the mail system. Finally, without the ability to adequately inspect excessive mail

---

[26] Prior to 2003, certain CBP functions were performed by U.S. Customs Service which authored this 2001 Handbook in use at the time of our audit.

[27] Designer drugs are illicitly produced as substances that differ slightly from controlled substances in their chemical structure while retaining their pharmacological effects.

FOR OFFICIAL USE ONLY

volumes from high-risk countries, highly lethal prohibited items, such as fentanyl, may proceed unexamined or tested and subsequently be disseminated in the United States.

Improvements Needed to CBP's Targeting and Interdiction of Prohibited Items in International Mail

Successful execution of CBP's targeting methodology and interdiction of prohibited items was hindered by multiple factors. According to CBP's ATS targeting database, CBP did not receive all targeted mail from the USPS. This was due in part to CBP's inability to accurately account for the mail provided by USPS, or ensure the mail was inspected. Additionally, CBP's targeting of mail for potential violations from October 1, 2018 through June 30, 2019 had a ███ percent detection rate due to a reliance on subjective expertise and incomplete advanced data. Given these challenges, CBP could not ensure all targeted mail was inspected prior to delivery.

CBP Did Not Receive All Targeted Mail It Requested from USPS

CBP's targeting methodology is contingent upon receipt of all mail it requests from USPS. CBP's ATS targeting database receives advance data and applies risk-based rules to identify high-risk mail pieces that may contain narcotics or other contraband. The prohibited items are flagged in CBP's ATS and transmitted electronically to USPS' Global Business System (GBS). According to the standard operating procedures among CBP, JFK, and the USPS, dated February 28, 2018, and other guidance,[28] USPS will strive to deliver 100 percent of targeted mail upon its arrival in the United States. CBP then relies on USPS staff to locate and transport the targeted packages to CBP personnel at the JFK IMF for inspection.

However, USPS did not always provide the targeted mail requested by CBP. To confirm this, we reviewed data from CBP's local MS Access Targeting Database of international mail parcels targeted for inspection at JFK from October 1, 2018 through June 30, 2019. Based on our analysis, CBP targeted ████ international mail packages that arrived at JFK during this timeframe.[29]

---

[28] *Standard Operating Procedures between U.S. Customs and Border Protection, John F. Kennedy International Airport, and the United States Postal Service, New York International Service Center Regarding Cooperation in the Inspection of Goods Imported or Exported through the Post,* February 28, 2018; *International Mail Operations and Enforcement Handbook* CIS HB-3200-06A, August 2001.

[29] While we are reporting on information in CBP's database, we also determined there were many errors in this database.
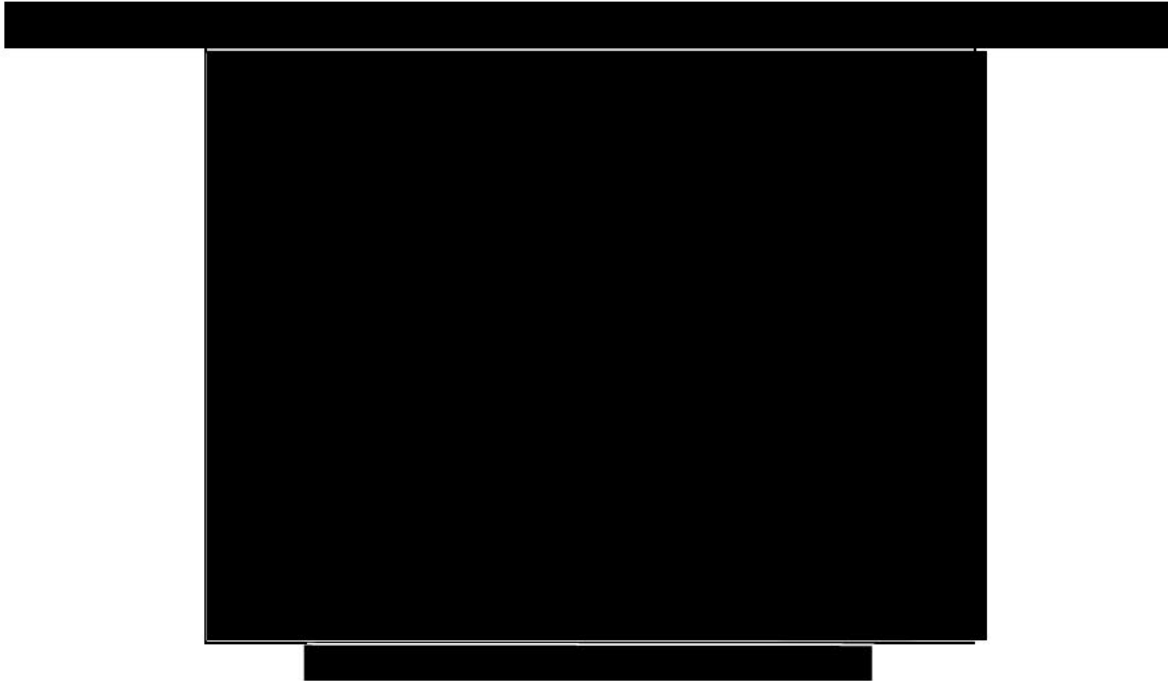
According to data from the local MS Access Targeting Database,[30] USPS did not provide ███████████████ of ██████ of the targeted packages, as shown in Figure 14.

CBP's Targeting Methodology Was Hampered by an Inability to Account for Targeted Mail from USPS

CBP stated that its ability to carry out effective targeting largely depends on the advanced data it received from USPS, as well as its ability to account for the targeted mail provided by USPS. However, CBP did not actually account for the targeted mail provided by USPS for inspection because it did not record or track each item received. This was because, according to CBP, if USPS did not provide the advanced data on the parcel, then it would not be in the CBP system for targeting. Also, CBP staff stated that USPS does not scan all items transferred to, or from, the CBP area at the JFK IMF.[31] Rather, targeted mail is only recorded when it is examined. Moreover, CBP personnel do not immediately look for the targeted mail because parcels may arrive later than their scheduled dates. CBP staff admitted it could take up to two weeks for CBP personnel to notice that targeted parcels had not been provided.

---

[30] We analyzed the MS Access Targeting Database and identified inadequate controls such as missing fields for exam time, exam date, violation type, and arrive date. There were no system checks to ensure data fields were required or complete. However, the database did have all the data fields we needed for quantifying targeted mail.

[31] We did not contact USPS to confirm CBP's assertion that USPS does not scan mail transferred into or out of the CBP area of the JFK IMF.

Additionally, CBP did not inventory inspected mail and packages received from USPS, or track whether the packages cleared for delivery were returned to USPS. According to CBP staff at JFK IMF, CBP only performed spot checks to verify whether requested mail was presented. CBP's standard operating procedure did not require inventory of targeted mail received from USPS. We asked CBP staff whether the procedure could be revised to require such inventory. However, CBP officials explained that targeted mail volumes are too large and USPS likely did not present all targeted mail for inspection as requested.

In our 2018 report, we stated that CBP did not inventory all mail requested from USPS because of the absence of updated guidance. We recommended CBP establish a process to inventory all arriving international air mail received from USPS, scanned by CBP, and returned to USPS. Although we followed up with CBP during this audit on its progress in establishing an inventory process, CBP had not yet finalized a process to resolve our recommendation.

CBP Targeting of Mail for Contraband Had a ▇ Percent Detection Rate

According to CBP, using advance data from its ATS system to identify inbound international items that may pose a threat to the United States enables them to detect prohibited items at higher rates. We determined that ▇ percent of the mail CBP targeted for inspection from October 1, 2018 through June 30, 2019 contained potential violations. Our analysis of CBP data showed that CBP identified potential violations in ▇▇▇▇▇▇▇▇ of the ▇▇▇▇ targeted packages presented by USPS, depicted in Figure 15.

We compared this finding with data reported by the JFK IMF to CBP's Office of Field Operations. CBP's trend analysis of international mail received and inspected at the JFK IMF for FY 2018 and the first half of FY 2019 illustrates that CBP examined only a percentage of all high-risk and targeted mail. Specifically, CBP examined ███████ percent of the mail from sources on the COI list, and less than ████████████████ of targeted mail, as illustrated in Table 1.

Table 1. OIG Analysis of CBP Data on Results of Its Examination of High-risk and Targeted Mail

Period	Parcels Received Per Year	Parcels Examined Per Day	Parcels Examined Per Year	Exam Rate	Parcels Containing Prohibited Items	Percent of Parcels Containing Prohibited Items
Random Examination of Mail from Countries of Interest						
FY 2018	365 million	████	████	██	██	█
FY 2019 (Oct. – Mar.)	180 million	████	████	██	██	█
Examination of Mail Targeted using Advanced Electronic Data						
FY 2018	365 million	█	██	██	██	██
FY 2019	180 million	█	██	██	██	██

Additionally, we determined that CBP did not specifically target mail that required duties and fees. CBP has a statutory responsibility to collect revenue owed to the U.S. Government from the importation of goods into the United States. Revenue collection is one of CBP's primary and recurring functions and was recently reclassified a Priority Trade Issue.[32] For example, an importer of record must pay CBP a merchandise processing fee for commercial goods valued at $2,500 or more.[33] However, CBP officers did not request high-risk mail that could require duties or fees upon entry in the United States

Inconsistent and Incomplete Data Hampered CBP's Target Detection

CBP officers we interviewed during our visit asserted that CBP's target detection rate is constrained by a reliance on subjective expertise and incomplete advanced data. These officers stated the advanced data in ATS further improves their ability to determine high risk parcels to target incoming mail from other countries. For example, advanced data officers in CBP's ATS Unit conduct targeting by relying on targeting thresholds or risk scores from ATS. However, CBP officers added that mail targeting can be hampered by incomplete advanced data because not all countries are required to provide the advanced data or do not provide complete contents of parcels to USPS.

Consequences of Mail Targeting Challenges

The limitations with targeted mail did not provide us with assurance that CBP physically inspects all targeted mail prior to delivery. Without tracking the targeted mail it receives, CBP is unaware of whether all mail in its possession is accounted for, and inspected, before being returned to USPS for delivery. As result, CBP will be unable to timely alert parties, such as the Food and Drug Administration, waiting to inspect the targeted mail. Moreover, CBP may be unaware of whether mail may be missing or stolen while in CBP's possession. In the meantime, CBP and USPS expend excessive time and resources searching and locating targeted mail for inspection. This mail is subsequently released to USPS when no import violation is found.

Without targeting mail subject to duties and fees, this could result in lost revenue to the United States. CBP is the second largest revenue source in the Federal Government, with the dual role of assisting trade and protecting revenue. Trade operations are focused on creating a level playing field for American businesses, protecting consumers, and reducing trade costs. Such

---

[32] *Trade Facilitation and Trade Enforcement Act of 2015,* 19 United States Code (U.S.C.) § 4322(a)(5) (2016).
[33] 19 C.F.R 24.23(b)(1).

~~FOR OFFICIAL USE ONLY~~

operations are placed at risk if shipments are imported into the United States without proper collection of duties and fees.[34]

Physical Security Controls to Safeguard International Parcels in CBP's Possession Needed Improvement

Physical security controls at the JFK IMF were inadequate to safeguard mail in CBP's possession. Specifically, CBP did not secure interior and exterior entrances and exits in the JFK IMF because existing staff procedures, according to CBP, negated the need for locked doors. CBP also did not have enough cameras to observe all exterior doors or areas where individual CBP staff processed mail. Deficient physical security controls could lead to unauthorized access to restricted areas, theft or misplacement of prohibited items, or staff's exposure to prohibited substances.

Lack of Physical Security for Entrances and Exits at JFK IMF

According to *DHS Sensitive Systems Policy Directive 4300A,*[35] access to DHS buildings, rooms, work areas, and spaces should be limited to authorized personnel. Moreover, controls for detecting and restricting access to sensitive areas should be in place to safeguard against possible loss, theft, and damage. *DHS Instruction Manual* on Physical Security[36] requires that tenants of multiple Federal organizations in a facility have a Facility Security Committee to establish physical access protocols (identification and screening) for employees, contractors, and visitors.

CBP did not adequately secure all interior and exterior doors in several JFK IMF mail processing areas. During our site visit, we observed that doors in all five mail holding areas remained unlocked, or potentially propped open, as pictured in Figures 16, 17, and 18. The unsecured areas contained tubs and pallets of mail waiting to be inspected; some of the mail contained illegal or harmful contents. Although we were unable to determine whether the doors were alarmed, JFK IMF staff confirmed that they were not.[37] We watched CBP and USPS staff enter and exit the holding areas freely through the unsecured doors. Additionally, one exit door in the CBP area of the JFK IMF was propped open and not alarmed.

---

[34] *CBP Trade and Travel Report*, January 2020.
[35] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017.
[36] *DHS Instruction Manual 121-01-010-01, Revision #01 Physical Security*, 7-21-14.
[37] Although alarms are not explicitly required in *DHS Sensitive Systems Policy Directive 4300A*, it prescribes that components have controls in place for detecting, restricting, and regulating access to sensitive areas.
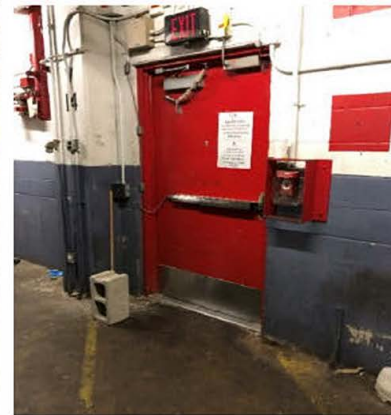
~~FOR OFFICIAL USE ONLY~~

Figure 16. Unsecured Registered Mail Cage

Figure 17. Enforcement Cage Door Propped Open

Figure 18. Exit Door with a Cinder Block Stopper

Source: OIG photos taken June 2019

CBP staff said they did not adequately secure all interior and exterior doors because they did not see the need for locked doors. According to CBP staff, the CBP area in the JKF IMF requires staff to use a key card to enter and exit through exterior doors. However, we saw non-CBP personnel move in and out of the sensitive areas without key cards. CBP also asserted that the interior doors to each mail holding area needed to remain unlocked to facilitate bringing in USPS containers and access by CBP personnel working in designated areas.

Insufficient Camera Coverage for Mail Inspection Areas at the JFK IMF

CBP's system of closed-circuit televisions (CCTV) did not provide sufficient visibility in the mail processing areas. During our June 2019 visit, we saw eight cameras within CBP's area of the JFK IMF. Several areas where CBP staff processed mail did not have adequate camera coverage, as shown in Figure 17. Specifically, there were no cameras in an enclosed, windowless room where a single CBP officer was inspecting letter mail. The cameras nearest the two unalarmed exit doors were not directed at the doors. JFK IMF staff were aware of the inadequate CCTV coverage and submitted a budget request to purchase additional CCTVs.

Figure 19.   CCTV Screens
Source: OIG photo taken June 2019

We questioned whether CBP would be aware if mail in its possession were to be removed from the facility without authorization. The absence of proper physical security controls could lead to unauthorized access to restricted areas; theft or misplacement of prohibited items; prohibited items improperly mailed to recipients; or staff exposure to prohibited substances. Inadequate physical security controls also increased the risk of insider theft. Specifically, since the doors were not alarmed, JFK IMF staff could access restricted sections of the mail processing area to steal mail containing prohibited items such as fentanyl. Individuals with malicious intent could also exit unalarmed doors with prohibited mail and management would be unaware of the breach.

CBP Controls over the IT Infrastructure and Systems Supporting Mail Processing Operations Were Ineffective

We identified several areas for improvement in CBP IT infrastructure supporting mail-processing operations at JFK IMF. CBP did not adequately patch an ATS server located in Springfield, VA. Also, a CBP database containing targeting information did not have adequate internal controls that could help ensure reliability. Lastly, CBP had not conducted the required privacy assessment on a database, known as the Unclaimed/Abandonment database, used to stored names and addresses of recipients for incoming international mail.

Server Supporting International Mail Processing Was Incorrectly Patched

According to the *DHS Sensitive Systems Policy Directive 4300A*,[38] components should ensure all recommended and approved security patches are properly installed. We conducted a technical scan of seven ATS servers at the JFK IMF in June 2019. We determined that CBP had not fully applied required system patches to one of the servers. Our technical scan identified four high-risk vulnerabilities because the patches had not been applied to the ATS server, even though CBP's own internal vulnerability scans had reported the error for several months.

The deficiency occurred because CBP did not correctly update an associated registry key to apply the patch appropriately.[39] According to a CBP official, CBP staff had not been instructed to review error logs to determine whether patches had been correctly applied. CBP should have investigated the patch implementation when the vulnerability previously appeared on monthly reports.

Without properly applying all recommended and approved security patches, CBP systems are vulnerable to malicious attacks. Systems with missing patches could lead to intruders attacking and gaining unauthorized access to systems, and obtaining and disclosing potentially sensitive information.

CBP's JFK Targeting Database Contained Inadequate Controls and Incomplete Data[40]

Federal guidance requires that applications be designed to process transactions accurately to ensure valid and complete data.[41] Controls should be established at an application's interfaces to verify inputs and outputs, such as edit checks.

Based on an internal initiative, CBP staff at the JFK IMF developed a temporary local MS Access Targeting Database application to help monitor international mail packages. According to a CBP official, the catalyst for developing the MS Access Targeting Database was the increasing number of mail violations and

---

[38] Version 13.1, July 27, 2017.

[39] The registry is a database of information, settings, options, and other values for software and hardware installed on Microsoft Windows operating systems. The registry key is updated through the Group Policy Objects, a policy setting in the file system and in the Active Directory.

[40] We analyzed the MS Access Targeting Database and identified inadequate controls such as missing fields for exam time, exam data, violation type, and arrive date. There were no system checks to ensure data fields were required or complete. However, the database did have all the data fields we needed for quantifying targeted mail.

[41] Office of Management and Budget Circular OMB-123.

limited staff to detect them. Previously, staff at the JFK IMF used targeting ledger books to record parcels that had been targeted. Furthermore, CBP officials stated that as each Targeter updates ATS with targets, they export the ATS information into the MS Access Targeting Database application. The CBP officials stated the Targeter also uses a handheld scanner to read the barcode of the targeted mail and update the MS Access Targeting database application to document that CBP received the targeted piece of mail.

CBP's MS Access Targeting Database did not contain controls to ensure valid and complete data is transferred over from ATS. Specifically, the database had missing or invalid key fields, such as "exam date," "violation type," "arrival date," and "exam time." To illustrate, we identified 1,551 records did not have valid arrival dates. In some cases, the database was also missing the source of referral, declared description, seizure number, and actual description. The database also contained errors. For example, we noted instances in which the exam date occurred before the mail arrival date. We identified 12,789 records that had no exam dates and 72 records exam date was before the arrival date.

Without reliable data, CBP may be unable to determine the effectiveness of its advanced targeting efforts or of USPS support. Furthermore, CBP staff may infer incorrect conclusions from the collection of incomplete data. CBP management of the international mail process cannot benefit from inaccurate statistics concerning the number of parcels targeted, the number provided by USPS, and the number found to contain prohibited items.

CBP Needed to Complete a Privacy Threshold Analysis on the Unclaimed/ Abandonment Database

According to DHS requirements,[42] information systems that collect, use, maintain, or disseminate personally identifiable information are subject to privacy compliance documentation. This includes a Privacy Threshold Analysis for submission to the DHS Privacy Office for review and approval for an information system to be designated as operational. The Privacy Threshold Analysis is also necessary for the Privacy Office to determine whether a Privacy Impact Analysis is needed. However, CBP has not conducted the required Privacy Threshold Analysis of its Unclaimed/Abandonment database, used to store names and addresses of recipients of incoming international mail. The Unclaimed/Abandonment database also contains information about personal use items such as medicines.[43] The data stored in the

---

[42] *DHS 4300A, Sensitive Systems Handbook* (Version 12.0, November 15, 2015) and *DHS Sensitive Systems Policy Directive 4300A* (Version 13.1 July 27, 2017).
[43] Personal use items are described as quantities too small to seize but still prohibited to deliver to the addressee.

Unclaimed/Abandonment database could be compromised absent the necessary security controls.

CBP did not conduct the required Privacy Threshold Analysis of the Unclaimed/Abandonment database because the database resided on the local area network at the JFK IMF. According to a CBP official at the JFK IMF, a Privacy Threshold Analysis was not required because the Unclaimed/Abandonment database is a stand-alone and local system. However, the DHS Privacy Office requires[44] systems to have a Privacy Threshold Analysis as a prelude to determining whether a Privacy Impact Analysis is also needed. Furthermore, a memorandum[45] issued by the Department on June 26, 2020, states that "even though systems are developed in the field to meet operational needs, it is important to implement security and privacy controls." The memorandum states "if a system lacks security and privacy documentation, it must be taken offline and brought into compliance with Federal policies."

Until CBP completes a Privacy Threshold Analysis of the Unclaimed/ Abandonment database, it may be placing personally identifiable information stored on the database at risk. Moreover, by not having adequate privacy documentation, CBP may be in violation of required privacy regulations.

Recommendations

We recommend the Acting Assistant Commissioner for the Office of Information Technology, and the Executive Assistant Commissioner for the Office of Field Operations, and Acting Executive Assistant Commissioner for Operations Support:

Recommendation 1: Provide the support staff and equipment necessary at the JFK IMF to adequately inspect mail in a timely manner.

We recommend the Executive Assistant Commissioner for the Office of Field Operations and Acting Executive Assistant Commissioner for Operations Support:

Recommendation 2: Ensure that information on seizure of prohibited substances or items at JFK IMF is recorded in SEACATS within 24 hours, as required.

---

[44] Privacy Threshold Analysis is required whenever a new information system is being developed or an existing system is significantly modified. PA9.m Adobe Page 80 Section 3.1.4.2
[45] *CBP Information System Security and Privacy Requirement*, June 26, 2019.

Recommendation 3: Conduct an analysis and revise the targeting methodologies as appropriate for JFK IMF to increase the effective rate of the mail targeting process.

Recommendation 4: Establish a process for JFK IMF to identify and reconcile targeted mail that is not provided by USPS.

Recommendation 5: Implement the necessary controls to secure mail in CBP's possession at the JFK IMF.

We recommend the Acting Assistant Commissioner for the Office of Information and Technology:

Recommendation 6: Create policy and procedures to ensure that all required system patches and registry keys are correctly applied.

We recommend the Executive Assistant Commissioner for the Office of Field Operations:

Recommendation 7: Develop a plan to improve the controls and reliability of the local database used to monitor targeted international mail.

We recommend the Acting Assistant Commissioner for the Office of Information and Technology, Executive Assistant Commissioner for the Office of Field Operations, and Acting Executive Assistant Commissioner for Operations Support:

Recommendation 8: Work with the DHS Privacy Office to ensure the Unclaimed/Abandonment database complies with DHS privacy policies.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Senior Component Accountable Official at CBP. In the comments, the Official stated CBP appreciates the recognition of its ability to screen large volumes of incoming international mail. However, CBP did not concur with all of our findings. The Official provided specific comments regarding each of CBP's concerns.

We reviewed CBP's comments, as well as the technical comments previously submitted under separate cover, and made changes to the report as appropriate. Following is our evaluation of CBP's general comments, as well as

a response to each recommendation in the draft report provided for agency review and comment.

OIG Response to General Comments

The Senior Component Accountable Official at CBP stated the OIG's draft report contained inaccurate and misleading statements, misrepresentations of facts and metrics, as well as misunderstandings and misrepresentations of CBP's staffing needs, effectiveness of SEACATS and other national systems, and global targeting methodology and processes. We disagree with this assertion. We ensured CBP was fully aware of the extent of the OIG's audit fieldwork and contacts with component personnel at the JFK IMF. Specifically, our project included meetings with CBP staff at the JFK IMF, including the Program Manager, Chief of Staff, Assistant Port Director, IMF Chief, agricultural staff, and canine staff, as well as CBP officials at the National Targeting Center. We assessed a compilation of CBP policies and procedures for processing, selecting, targeting, examining, and interdicting inbound international mail at JFK. We also observed CBP staff operations, mail inspection equipment, and JFK facilities. We believe the range of audit information compiled was a sound and ample basis from which to form our audit conclusions and recommendations.

Further, the Senior Component Accountable Official at CBP stated the OIG lacked understanding of CBP's targeting, screening, and processing strategies and methodologies. The Official explained that CBP employs a layered approach using numerous methods to identify packages for inspection, including analysis of advanced electronic data through an automated targeting system, narcotics detection canines, and non-intrusive inspection technologies. We find this assertion inconsistent with our report, which clearly states, "CBP has a multi-layered approach for scanning and inspecting international airmail at the JFK IMF. This 3-tier approach includes: (1) intelligence gathering for advanced mail targeting, (2) x-ray machine inspection and canine inspection, and (3) CBP's physical inspection and testing of mail contents." (*See* page 3 of our report).

Response to Report Recommendations

In the formal written comments, the Senior Component Accountable Official at CBP concurred with recommendations 2, 4, 5, 6, 7, and 8, but did not concur with recommendations 1 and 3. A copy of CBP's responses in its entirety is included in Appendix B. A summary of CBP's response to each recommendation and OIG's analysis follows.

CBP Comments to Recommendation 1: Non-concur. Regarding staffing, the Senior Component Accountable Official said CBP's limited resources mitigate threats in all environments. The CBP Office of Field Operations Workload Staffing Model estimates a staffing shortage of 2,000+ CBP officers across the Nation, throughout all environments, including mail facilities. CBP continuously evaluates and adjusts its limited staff resources to effectively meet all its mission needs, including timely inspection of mail at the JFK IMF, as appropriate.

Regarding equipment at the JFK IMF, CBP has initiated several equipment and facility-related projects to modernize the JFK IMF. CBP commissioned a feasibility study to be conducted for the JFK IMF during FY 2020, including assessment of structure, equipment and potential future needs. In addition, CBP has received funding to update the current infrastructure and technology at the JFK IMF. Enhancements include the installation of mail sorting equipment to increase operational efficiency and allow CBP to screen a larger portion of international mail than is currently being processed. The estimated completion date is November 30, 2021.

OIG Analysis of CBP Comments: We agree with CBP's plan to conduct the feasibility study of the structure, equipment and potential future needs at the JFK IMF. We also encourage CBP to conduct a similar study or analysis of the staffing levels at the JFK IMF. We made similar recommendations, to which CBP concurred, in our prior audit report, *CBP's International Mail Inspection Processes Need Improvement at JFK International Airport,* (OIG-18-83) in which we requested that CBP conduct an analysis of staffing levels at the JFK IMF.

Given CBP's non-concurrence, we consider this recommendation open and unresolved.

CBP Comments to Recommendation 2: Concur. CBP's *Seized Asset Management and Enforcement Procedures Handbook* (HB 4400-01B) already has multiple sections outlining the requirements for capturing and recording information pertaining to seizures of prohibited substances within 24 hours. In addition, SEACATS, CBP's law enforcement system of record, has a system of internal checks in place to notify case initiators and supervisors of actions pending completion associated with these seizures. CBP will provide supporting documentation under separate cover. CBP requested that OIG consider this recommendation resolved and closed as implemented.

OIG Analysis of CBP Comments: We do not consider the actions outlined to be responsive to the recommendation. We recommended CBP ensure the information about seizure of prohibited substances or items at JFK IMF be recorded in SEACATS within 24 hours, as required. We are aware that CBP's

Seized Asset Management and Enforcement Procedures Handbook (HB 4400-01B) already contains requirements for capturing and recording information pertaining to seizures of prohibited substances within 24 hours.

We encourage CBP to revise, as appropriate, its approach for ensuring CBP personnel at the JFK IMF comply with requirements for recording information pertaining to seizures of prohibited substances within 24 hours. This recommendation is open and unresolved until CBP can provide an estimated completion date.

CBP Comments to Recommendation 3: Non-concur. CBP was troubled that this recommendation indicated a misunderstanding of how it targets across the inbound and outbound cargo environments. CBP continuously evaluates, refines and implements targeting methodologies across its mission sets, including, but not limited to, the international mail environment. CBP requested that OIG consider this recommendation resolved and closed as implemented.

OIG Analysis of CBP Comments: We do not agree with CBP's response to this recommendation. During the audit, we reviewed targeting data from CBP's ATS targeting database identifying that not all of the targeted mail from USPS was received. In addition, we reviewed data from CBP's local MS Access Targeting Databases on international mail parcels targeted for inspection and determined USPS did not always provide the targeted mail CBP requested. CBP staff at the JFK IMF informed us that they were unable to account for the targeted mail provided by USPS for inspection because CBP did not record or track each item received.

We recognize CBP's use of advance data from its ATS to identify high-risk inbound international items. However, we determined that ██ percent of the targeted mail actually contained potential violations. We concluded this was because of a reliance on subjective expertise and incomplete advanced data. This recommendation is open and unresolved.

CBP Comments to Recommendation 4: Concur. CBP Office of Field Operations' New York Field Office will review the existing process for identifying and reconciling mail that is electronically targeted by CBP, but not presented by USPS to CBP for examination. The office will collaborate with USPS at JFK to enhance this process. Completion of the New York Field Office's review of an enhanced process will be dependent on the outcome of the CBP Office of Information and Technology's development of a plan to improve reliability of the database used to monitor targeted international mail. The estimated completion date is July 31, 2021.

OIG Analysis of CBP Comments: CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation showing that all planned corrective actions are completed.

CBP Comments to Recommendation 5: Concur. CBP Office of Field Operations will implement security measures necessary to secure mail in CBP's possession at the JFK IMF. These measures include a review of security policies and practices, training materials, quarterly reviews of policies and procedures effectiveness, and tracking of the security of mail in CBP's possession. The estimated completion date is June 30, 2021.

OIG Analysis of CBP Comments: CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation showing that all planned corrective actions are completed.

CBP Comments to Recommendation 6: Concur. The CBP Office of Information Technology demonstrated the patch to the server in question had already been applied and existing policies and procedures for patch deployment were followed. However, the office acknowledged the same server was missing a registry entry at the time because the automated group policy orchestrator encountered a communication problem with the host. The Office of Information Technology will make it a priority to institute verification of the successful application of group policy orchestrator policies on a more frequent and ongoing basis so that anomalies like this are detected and addressed earlier. Specifically, the office will more proactively communicate with Windows Admins to identify failures in registry key updates and group policy orchestrator failures and will continue its semi-monthly Nessus scan result reviews on the Windows servers with peer verification. The estimated completion date is March 31, 2021.

OIG Analysis of CBP Comments: CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation showing that all planned corrective actions are completed.

CBP Comments to Recommendation 7: Concur. The Office of Field Operations' New York Field Office will develop an action plan to address reliability of the database used to monitor targeted international mail. This effort will include evaluating the tracking database to determine which, if any, data elements should continue to be gathered, or whether the database should be discontinued. The estimated completion date is April 30, 2021.

OIG Analysis of CBP Comments: CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation showing that all planned corrective actions are completed.

CBP Comments to Recommendation 8: Concur. CBP's Office of Field Operations Cargo and Conveyance Security, New York Field Office, Office of Information and Technology, Chief Counsel, and the Privacy and Diversity Office will evaluate the Unclaimed/Abandonment database to bring it into compliance with DHS' privacy policy or identify an existing system of record capable of capturing the necessary data. The estimated completion date is April 30, 2021.

OIG Analysis of CBP Comments: CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation showing that all planned corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*. We conducted this audit to determine whether CBP's airmail, physical security, and inspection processes at JFK International Airport IMF are adequate to effectively screen, track, and safeguard incoming international mail.

To accomplish our audit objective, we reviewed CBP policies and procedures for processing, selecting, targeting, examining, and interdicting inbound international mail at JFK. Specifically, we reviewed the MOU and standard operating procedures to determine roles, responsibilities, and agreements between CBP and USPS. We also reviewed floor plans to assess space allocation between CBP and USPS and determine where international mail is stored before and after inspection. We reviewed internal controls and protocols for ATS security to verify the completeness and accuracy of the data it produces. We assessed the adequacy of physical controls necessary for CBP to safeguard international mail suspected of containing contraband at JFK IMF.

We coordinated with staff from USPS OIG to assist us in this effort. We obtained from USPS an inventory of mail arriving at the JFK IMF during June 2019. USPS personnel extracted the data from its GBS. We obtained from USPS the specific mail pieces CBP requested for inspection based on the COI list and the individual mail pieces that were targeted. While we did not directly test the reliability of this data, we obtained a statement from the USPS to attest that the GBS data was reliable. Furthermore, we reviewed the USPS' *Advance Electronic Data Holds and Reliability[46]* report to gain understanding of how USPS test the reliability of its data generated from USPS' systems. We also interviewed USPS OIG officials who were knowledgeable about the data. Lastly, our Data Analytics team reviewed the data for completeness and obvious inconsistency errors, and identified insignificant errors in the raw data. We determined that the data was sufficient for the audit.

To gain an understanding of the international mail inspection process, roles, and responsibilities, we met with selected CBP officials, such as CBP cargo staff at the National Targeting Center in Sterling, VA. Additionally, we conversed with the information system security manager and the technology specialist with management oversight of ATS in Northern Virginia. We visited

---

[46] Office of Inspector General USPS, *Advance Electronic Data Holds and Reliability*, Report Number MS-AR-19-002, July 12, 2019

the JFK IMF to evaluate inspection equipment, processes, and physical security. We interviewed CBP staff, including the program manager, chief of staff, assistant port director, IMF chief, agricultural staff, and canine staff at the JFK IMF. We observed CBP officials performing technical scans on ATS servers at the component's Springfield, Virginia data center. Further, we followed up on the status of CBP's corrective actions to address deficiencies identified from our previous audit.

We used the work of specialists from the DHS OIG Information Assurance and Testing Branch to determine whether servers supporting JFK mail inspection meet IT security control requirements and DHS standards. The specialists completed the following:

- Performed a Defense Information Systems Agency Security Technical Implementation Guide configuration management assessment on all servers within the CBP ATS system authorization boundary.
- Performed a patching vulnerability assessment on all servers within the CBP ATS system authorization boundary.
- Performed a scan to identify unsupported operating systems on all CBP ATS servers assessed.

The results of their work are incorporated as appropriate in our findings. We also used the work of specialists from the DHS OIG-Wide Analytics and Support, who assisted the audit team with reviewing and analyzing data records from USPS, and CBP's ATS data, and presenting the information graphically. The results of their work are incorporated as appropriate in our findings.

We conducted this performance audit between May 2019 and February 2020 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 the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the efforts of CBP management and staff to provide the information and access necessary to accomplish this audit. Major OIG contributors to the audit are identified in Appendix C.

Appendix B
CBP Comments to the Draft Report

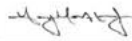1300 Pennsylvania Avenue NW
Washington, DC 20229

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

September 1, 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

X ~~signature~~   9/1/2020

Signed by: HENRY A MOAK JR

SUBJECT: Management Response to Draft Report: "CBP Inspection
Processes and Physical Security are Inadequate to Effectively
Screen Mail at the JFK International Mail Facility"
(Project No. 19-050-AUD-CBP)

Thank you for the opportunity to comment on this draft report. The 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 appreciates the OIG's recognition of its ability to screen large volumes of incoming
international mail, while executing its critical role in the interdiction of dangerous
substances and prohibited items, including opioids, at U.S. international airports and mail
facilities. CBP's highest priority in screening inbound international mail is to prevent
terrorists' weapons and other harmful items from entering the United States, including
taking actions to identify such threats prior to the item actually arriving in the United
States. CBP remains committed to maintaining safe and efficient mail screening
facilities.

CBP is seriously concerned that, despite multiple meetings with subject matter experts to
explain and clarify information, the OIG's draft report contains many inaccurate and
misleading statements, numerous misrepresentations and mischaracterizations of facts
and metrics, and misunderstandings and misrepresentations of CBP's staffing needs,
effectiveness of the Seized Asset and Case Tracking System (SEACATS) and other
national systems, and global targeting methodology and processes. The OIG's clear lack
of understanding of CBP's targeting, screening and processing strategies and
methodologies has led to a fundamentally flawed report that is based on erroneous
judgements and assumptions.

To make admissibility determinations, CBP employs a layered approach using numerous methods to identify packages for inspection to include, analysis of Advance Electronic Data (AED) through an automated targeting system, narcotics detection canines, and non-intrusive inspection technologies. In addition, CBP officers manually select packages for additional scrutiny based on extensive experience and knowledge garnered through lengthy tenures working in the international mail and other cargo environments. The OIG's draft report offers opinions and judgments that infer these processes are inefficient and ineffective, when the data and subject matter experts come to the exact opposite conclusions.

The draft report contained eight recommendations, with which CBP concurs with six (Recommendations 2, 4, 5, 6, 7, and 8), and non-concurs with two (Recommendations 1 and 3. Attached find our detailed response to each recommendation. CBP previously submitted technical comments under a separate cover for OIG's consideration.

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

2

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Attachment: Management Response to Recommendations
Contained in OIG-19-050-AUD-CBP

OIG recommended that the Assistant Commissioner for the Office of Information and Technology and the Executive Assistance Commissioner for Field Operations and Operations Support:

Recommendation 1: Provide the support staff and equipment necessary at the JFK IMF [John F. Kennedy International Mail Facility] to adequately inspect mail in a timely manner.

Response: Non-concur. This recommendation has two distinctly separate components: 1) Staffing and 2) equipment. Regarding staffing, CBP's limited resources mitigate threats in all environments. The CBP Office of Field Operations (OFO) Workload Staffing Model estimates a staffing shortage of 2,000+ CBP officers across the Nation, throughout all environments, including mail facilities. CBP continuously and judiciously evaluates and adjusts its limited staff resources to effectively meet all its mission needs, including the timely inspection of mail at the JFK IMF, as appropriate.

Regarding equipment, CBP has initiated several equipment and facility-related projects to modernize the JFK IMF. For example, in January 2020, CBP Enterprise Services, Office of Facilities and Asset Management commissioned a feasibility study to be conducted of the JFK IMF during fiscal year 2020, to include structure, equipment and potential future needs. In addition, CBP has received funding to update the current infrastructure and technology at the JFK IMF. Enhancements include the installation of mail sorting equipment that will increase the efficiency of operations, and allow CBP to screen a larger portion of international mail than is currently being processed. This increase in screening will also be combined with innovative non-intrusive inspection (NII) technology. Estimated Completion Date (ECD): November 30, 2021

OIG recommended that the Executive Assistant Commissioners for Field Operations and Operations Support:

Recommendation 2: Ensure that information on seizure of prohibited substances or items at JFK IMF is recorded in SEACATS within 24 hours, as required.

Response: Concur. CBP's Seized Asset Management and Enforcement Procedures Handbook (HB 4400-01B) already has multiple Sections that clearly outline the requirements for capturing and recording information pertaining to seizures of prohibited substances within 24 hours. In addition, SEACATS, CBP's law enforcement system of record, has an internal system of checks in place that notify case initiators and

3

www.oig.dhs.gov 38 OIG-21-27

supervisors of actions pending their completion associated with these seizures. Supporting documentation will be provided under separate cover.

CBP request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 3: Conduct an analysis and revise the targeting methodologies as appropriate for JFK IMF to increase the effective rate of the mail targeting process.

Response: Non-concur. CBP is troubled that this recommendation indicates a clear misunderstanding by the OIG of how CBP targets across the inbound and outbound cargo environments. CBP continuously evaluates, refines and implements refined targeting methodologies across our mission sets, including, but not limited to, the international mail environment. More specifically, CBP:

- Uses a multi-layered risk approach, which it continuously reviews and updates to respond to evolving threats and trends,
- Coordinates with U.S. industries, 47 federal agency partners, and foreign governments to detect anomalies, trends, and violations in the global supply chain, to target high-risk shipments and promote compliance,
- Uses state-of-the-art technology and highly skilled targeting specialists to target and coordinate examination of high-risk shipments, while permitting legitimate trade to flow unimpeded,
- Takes in large amounts of advanced data and uses sophisticated targeting tools and subject-matter expertise to analyze, assess, and segment risk at every stage in the supply chain, and
- Leverages classified, law enforcement, commercial, and open-source information in unique, proactive ways to identify high-risk shipments at the earliest possible point before arrival in the United States.

CBP's analysis and information activities are used not only to stop potentially dangerous inbound shipments, but also to inform longer-term investigations into bad actors behind those shipments. The key to these targeting efforts is the data CBP collects.

It is also important to note that as CBP moves closer to 100 percent advance electronic data collection as required by the STOP Act, CBP's effectiveness in the mail environment will also increase. An essential element of CBP's layered security strategy is obtaining advance information to help identify shipments that are potentially at a higher risk of containing contraband.

4

CBP request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 4: Establish a process for JFK to identify and reconcile targeted mail that is not provided by USPS [United States Postal Service].

Response: Concur. CBP OFO's New York Field Office (NYFO) will review the existing process for identifying and reconciling mail that is electronically targeted by CBP, but not presented by USPS to CBP for examination, and will collaborate with USPS at JFK to enhance this process. The completion of the NYFO review and enhanced process will be dependent on the outcome of the CBP Office of Information and Technology's (OIT) development of a plan to improve the reliability of the database used to monitor targeted international mail. ECD: July 31, 2021

Recommendation 5: Implement the necessary controls to secure mail in CBP's possession at the JFK IMF.

Response: Concur. CBP OFO will implement security measures necessary to secure mail in CBP's possession at the JFK IMF by:

- Conducting a review of all pertinent CBP security policies and practices at the JFK IMF;
- Updating the security policies accordingly, and include a method for an appropriate management official to record/track that the security policies are being followed on a daily basis;
- Issuing appropriate training materials to all CBP JFK IMF employees regarding security policies and practices; and,
- Conducting quarterly reviews of the security policies and procedures effectiveness and the tracking thereof and adjust accordingly to ensure the security of the mail in CBP's possession.

ECD: June 30, 2021

OIG recommended that the Assistant Commissioner for the Office of Information and Technology:

Recommendation 6: Create policy and procedures to ensure that all required system patches and registry keys are correctly applied.

Response: Concur. As CBP OIT demonstrated during the audit fieldwork, the patch to the server in question had already been applied. Thus, existing procedures and policies for patch deployment were followed. Nessus scans are run twice monthly on the

5

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Windows servers which support JFK's mail processing facility. All Patches were implemented on these servers. However, OIT acknowledges that the same server was missing a registry entry at that time because the automated group policy orchestrator (GPO) encountered a communication problem with the host. OIT will make it a priority to institute a verification of the successful application of GPO policies on a more frequent and ongoing basis so that anomalies like this are detected and addressed earlier. Specifically, OIT will be more proactive communicating with Windows Admins in identifying failures in registry key updates and GPO failures and will continue its semi-monthly Nessus scan result reviews on the Windows servers with peer verification. ECD: December 31, 2020

Recommendation 7: Develop a plan to improve the reliability of the database used to monitor targeted international mail.

Response: Concur. The OFO NYFO will develop an action plan to address reliability of the database used to monitor targeted international mail. The action plan will include evaluating the tracking database to determine the which, if any, data elements should continue to be gathered, or whether the database should be discontinued. ECD: April 30, 2021

OIG recommended that the Assistant Commissioner for the Office of Information and Technology and Commissioners for Field Operation and Operations Support:

Recommendation 8: Work with the DHS Privacy Office to ensure the Unclaimed/Abandonment database complies with DHS privacy policies.

Response: Concur. The CBP offices of OFO Cargo and Conveyance Security, NYFO, OIT, Chief Counsel, and the Privacy and Diversity Office will evaluate the Unclaimed / Abandonment database to bring it into compliance with DHS' privacy policy or identify an existing system of record capable of capturing the necessary data. The later outcome would result in use of the Unclaimed / Abandonment databased being discontinued. ECD: April 30, 2021

6

www.oig.dhs.gov   41   OIG-21-27

Appendix C
Office of Audits Major Contributors to This Report

Kevin Burke, Director, Information Systems and Controls
Charles Twitty, Supervisory IT Auditor
Sonya Davis, Senior IT Auditor
Raheem Wilson, Program Analyst
Robert Williams, Senior Program Analyst
Donna Zavesky, IT Auditor
Stephen Wheeler, Program Analyst, OIG-Wide Analytics and Support
Ruksana Lodi, Program Analyst, OIG-Wide Analytics and Support
Mai Huynh, Program Analyst, OIG-Wide Analytics and Support
Thomas Rohrback, Branch Chief, Information Assurance and Testing
Jason Dominguez, IT Specialist, Information Assurance and Testing
Taurean McKenzie, IT Specialist, Information Assurance and Testing
Rashedul Romel, IT Specialist, Information Assurance and Testing
Richard Joyce, Independent Referencer
Gary Alvino, Independent Referencer
Deborah Mouton-Miller, Communications Analyst

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
Commissioner of CBP
CBP Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees