United States Government Accountability Office

Report to Congressional Committees

July 2021

AIR CARGO SECURITY

TSA Field Testing Should Ensure Screening Systems Meet Detection Standards

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-105192

GAO@100 Highlights

Highlights of GAO-21-105192, a report to congressional committees

July 2021

AIR CARGO SECURITY

TSA Field Testing Should Ensure Screening Systems Meet Detection Standards

Why GAO Did This Study

According to DHS—which is responsible for ensuring the security of air cargo transported to the United States—the threat from explosives in air cargo remains significant.

The TSA Modernization Act includes a provision for GAO to review DHS's processes for securing U.S.-bound air cargo and efforts to use CT technology for air cargo screening. This report addresses, among other things, how DHS secures inbound air cargo, and the extent to which TSA's field assessment of a CT screening system included key practices for design and evaluation.

GAO reviewed TSA and CBP air cargo security procedures and documents and analyzed a random sample of air cargo shipment data from calendar year 2019. GAO also interviewed TSA and CBP headquarters and National Targeting Center officials, and interviewed TSA field and air carrier officials regarding operations with two foreign airports, selected based on TSA risk data and the amount of air cargo transported from these airports to the United States. This is a public version of a sensitive report that GAO issued in May 2021. Information that DHS deemed sensitive was omitted.

What GAO Recommends

In the May 2021 report, GAO made four recommendations, including that TSA ensure it collects all necessary data for field assessments of explosives detection systems for air cargo screening prior to qualifying the systems for use by air carriers. DHS agreed with all four recommendations and said TSA and CBP are taking or planning actions to address them.

View GAO-21-105192. For more information, contact Triana McNeil at (202) 512-8777 or mcneilt@gao.gov or Karen L. Howard at (202) 512-6888 or howardk@gao.gov.

What GAO Found

The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) and U.S. Customs and Border Protection (CBP) address U.S.-bound air cargo security through separate programs and have taken steps to measure their effectiveness. For example, TSA conducts an inspection program to help ensure that air carriers comply with specific cargo-related security requirements, such as requirements related to cargo acceptance, control and custody, and screening procedures.

Air Cargo Pallet and Air Cargo Loaded onto an Aircraft

Source: GAO. | GAO-21-105192

From January 2020 through April 2021, TSA conducted a field assessment on the use of a computed tomography (CT)-based explosives detection system to screen air cargo as part of its ongoing process to qualify the system for use by air carriers. This type of system produces images of parcels that are examined by computer for signs of explosives. However, TSA's assessment did not fully meet three of five key design and evaluation practices. While the assessment identified goals and established metrics, TSA did not incorporate other key practices, such as collecting all necessary data about the system's ability to detect threats (probability of detection) in the field, consistent with TSA's standards. Since TSA officials cannot use live explosives in the field to measure the probability of detection, they relied on image quality testing, using a manufacturer's test kit to compare system performance in the field with earlier tests performed in a laboratory with live explosives.

However, TSA did not validate that the test kit was an acceptable alternative test method for determining the CT system's probability of detection in the field. TSA did not (1) independently validate that the test kit captures all ways system performance could degrade or (2) collect any of the underlying quantitative data from the test kit. TSA officials told GAO they did not validate the test kit because its performance was certified during laboratory testing at DHS's Transportation Security Laboratory; however, officials from the Transportation Security Laboratory told GAO they do not certify the performance of test kits. Without a suitable alternative testing approach to determine the probability of detection, TSA will not have all relevant data to assess whether the CT system meets TSA's detection standard requirements in the field and should be qualified for use by air carriers.

Contents

Figures

Abbreviations

ACAS	Air Cargo Advance Screening
ADIAC	Aviation Domain Intelligence Integration and Analysis Cell
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
CBP	U.S. Customs and Border Protection
CT	computed tomography
DHS	Department of Homeland Security
ICAO	International Civil Aviation Organization
NCSP	National Cargo Security Program
ROC	Receiver Operating Characteristic
TSA	Transportation Security Administration

441 G St. N.W.
Washington, DC 20548

July 29, 2021

Congressional Committees

The Department of Homeland Security (DHS) considers the security threat posed by terrorists attempting to conceal explosives in air cargo shipments to remain significant. In July 2017, a terrorist group shipped partially assembled components of a bomb from Turkey to Australia with plans to detonate the assembled device on a passenger flight. Seven years earlier, al-Qaeda attempted to conceal explosives in printer cartridges on a U.S.-bound flight from Yemen to Chicago. In fiscal year 2017, about 13 billion pounds of cargo was transported to the United States by aircraft. The air transportation industry forecasts that worldwide air cargo volume will grow by approximately 13 percent in 2021.[1]

DHS's Transportation Security Administration (TSA)—the federal agency with primary responsibility for securing the nation's civil aviation system—has programs in place to help ensure the security of passengers and property, including cargo, transported on U.S.-bound flights.[2] TSA's responsibilities for cargo transported on U.S.-bound flights include establishing security requirements governing U.S. and foreign-flagged air carrier operations and overseeing implementation of such requirements. U.S. Customs and Border Protection (CBP), also a component of DHS, is responsible for facilitating legitimate trade and travel at our nation's borders while keeping terrorists and their weapons, criminals and contraband, and other inadmissible individuals and goods out of the country. In 2010, in response to the al-Qaeda printer cartridge plot, TSA and CBP initiated the Air Cargo Advance Screening (ACAS) program to more readily identify high-risk cargo on passenger and all-cargo aircraft

[1]According to the International Air Transport Association—a trade association for airlines that states it represents 82 percent of total air traffic—in 2020 worldwide air cargo accounted for a much larger share of airlines' overall activities, due to a drop in passenger volume brought on by the COVID-19 pandemic. The association reported in January 2021 that industry-wide air cargo volume, after dropping in 2020 due to the COVID-19 pandemic, rose above pre-COVID-19 levels to approximately 1 percent over the January 2019 level.

[2]See generally Pub. L. No. 107-71, 115 Stat. 597 (2001); 49 U.S.C. §§ 114, 44901; 49 C.F.R. ch. XII, subch. C (pts.1540-1562); 6 U.S.C. §§ 203, 233, 234.

bound for the United States. CBP and TSA use ACAS to review air carriers' air cargo manifest data prior to loading the cargo.

The TSA Modernization Act, enacted as part of the Federal Aviation Administration Reauthorization Act of 2018 (the Act), includes a provision for us to review DHS's efforts to secure U.S-bound air cargo in the areas of prescreening processes and procedures, DHS's risk-based strategy for examining air cargo, TSA's pilot program on the use of computed tomography (CT) technology to screen air cargo, and DHS's information-sharing procedures and practices.[3]

This report

1. Identifies the DHS programs that address U.S.-bound air cargo security and discusses how DHS measures their effectiveness;
2. Examines how DHS's ACAS program identifies high-risk U.S.-bound air cargo shipments;
3. Assesses the extent to which TSA and CBP have a documented process to ensure the full exchange of relevant information for assessing risk to inbound air cargo;
4. Assesses the extent to which TSA's air cargo CT field assessment incorporated key practices for program design and evaluation; and
5. Identifies CBP and TSA's information-sharing procedures and practices for sharing threat information related to U.S.-bound air cargo with relevant stakeholders.

[3]Title I of Division K of the Federal Aviation Administration Reauthorization Act of 2018, Pub. L. No. 115-254, div. K, title I, subtitles B & D, §§ 1925 (Computed Tomography Pilot Programs), 1945 (GAO Review), 132 Stat. 3186, 3563-64, 3584-85. Although the Act refers to TSA conducting a "pilot program" on the use of technology to screen air cargo, for the purposes of this report we use the term "field assessment," which is TSA's preferred terminology to refer to the efforts undertaken to address the statutory directive.

In accordance with the Act, we conducted this review and provided relevant Congressional committees with an overview of our preliminary findings in the fall of 2020.[4]

This report is a public version of a sensitive report we issued on May 13, 2021.[5] DHS determined some information in our May report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information regarding the (1) foreign international airports we selected, (2) security-related vulnerabilities TSA identified at foreign airports worldwide, (3) U.S. and foreign-flagged air carriers we contacted, (4) TSA field offices that work with the U.S. and foreign-flagged air carriers we contacted, and (5) risk assessment tools DHS uses in its ACAS program to identify high-risk U.S.-bound air cargo shipments. Although we have omitted such sensitive information, this report addresses the same objectives—identified above—as the sensitive report and uses the same methodology.

To identify which DHS programs address U.S.-bound air cargo security, we reviewed TSA and CBP documentation that detail requirements for passenger and all-cargo air carriers (both foreign and U.S.-flagged) that transport cargo into the United States.[6] We also reviewed TSA security directives and emergency amendments related to air cargo. We interviewed TSA and CBP officials regarding (1) TSA's air cargo security requirements for the various classes of air carriers, (2) TSA's National Cargo Security Program (NCSP) Recognition Program, (3) TSA's air

[4]Pub. L. No. 115-254, § 1945, 132 Stat. at 3584. The Act directs us to conduct our review not later than 2 years after enactment (Oct. 5, 2020). We provided, or offered to provide, our preliminary findings to three oversight committees: U.S. Senate Committee on Commerce, Science and Transportation; the U.S. Senate Committee on Homeland Security and Governmental Affairs; and the U.S. House Committee on Homeland Security.

[5]GAO, *Air Cargo Security: TSA Field Testing Should Ensure Screening Systems Meet Detection Standards*, GAO-21-339SU (Washington, D.C.: May 13, 2021).

[6]Air cargo includes freight and express packages that range in size from small to very large, and in type from perishables to machinery, and can include items such as electronic equipment, automobile parts, clothing, medical supplies, other dry goods, fresh cut flowers, fresh seafood, fresh produce, tropical fish, and human remains. Cargo can be shipped in various forms, including large containers known as unit loading devices that allow many packages to be consolidated into one container that can be loaded on an aircraft, wooden crates, assembled pallets, or individually wrapped/boxed pieces, known as "break-bulk" cargo.

carrier inspection program, (4) TSA's airport assessment program, and (5) CBP's ACAS Program.[7]

For the ACAS program, we obtained air cargo summary data for fiscal years 2017 through 2020 on data submitted by air carriers, the number of submissions CBP reviewed, and CBP referrals to air carriers (for actions to be taken).[8] We chose these fiscal years because they covered the end of the ACAS pilot period and the first 2 years of full implementation. We also assessed the reliability of data contained in the ACAS module of CBP's Automated Targeting System (ATS) database. ATS is a decision-support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based assessments.[9] We concluded that the ACAS data contained in the ATS database were sufficiently reliable for our purposes of showing the level of program activity.

To obtain insight on the application of TSA and CBP air cargo security programs and requirements from the industry perspective, we selected two foreign international airports as a starting point for selecting air carriers to interview.[10] We selected these two airports based on (1) TSA's assessment of risk for these airports and (2) the amount of cargo transported from these airports to the United States (i.e., these airports were among the top 25 worldwide in fiscal year 2017 for transporting air cargo into the United States). We reached out to a total of 12 domestic and foreign-flagged air carriers and interviewed 11 of them.[11] Nine of the

[7]Foreign governments also establish national cargo security programs (NCSP) and may impose their own security requirements on air cargo operations within their jurisdictions—including screening requirements that may differ from TSA-established requirements—which apply to air cargo bound for the United States from their airports. Through its NCSP Recognition Program, TSA analyzes the air cargo security programs of its foreign counterparts and determines if a country's security program is commensurate with the level of security required under U.S. air cargo security programs.

[8]Throughout this report, we use the term "air carriers" to refer to both passenger and all-cargo air carriers that transport air cargo into the United States.

[9]According to CBP officials, ATS compares existing information on individuals and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns—or risk assessments—are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence corroborating those trends. We have omitted the details of the risk assessments because CBP deems them to be sensitive.

[10]Because TSA deems the identity of these foreign international airports to be sensitive, we have omitted their names and geographic locations.

[11]One of the 12 carriers did not respond to our requests for an interview. We interviewed 10 air carriers by telephone and one through email.

12 carriers transported cargo from one or both of the foreign international airports to the United States. We contacted three additional carriers that, based on fiscal year 2017 Bureau of Transportation Statistics data, did not transport cargo from these two airports to the United States but were major air carriers worldwide, including the transport of cargo to the United States.

We also reviewed applicable TSA summary compliance results for the two airports to gain insight into the agency's compliance operation and air carriers' level of compliance with air cargo security requirements. We determined that these data were sufficiently reliable for our purposes. In addition, we interviewed TSA field personnel responsible for compliance and coordination with air carriers and local governments at these airports for their perspective on the agency's compliance operations and carriers' level of compliance.

To determine how TSA and CBP measure the effectiveness of air cargo security programs and requirements, we reviewed performance data reports and interviewed officials regarding performance measures and compliance data TSA is tracking in response to our prior recommendations for the air carrier inspection, foreign airport assessment, and NCSP Recognition programs.[12] We also interviewed TSA officials about the agency's covert testing at overseas airports to assess compliance with air cargo security requirements and reviewed the status of CBP's efforts to monitor ACAS program performance.

To examine how CBP's ACAS program identifies and assesses high-risk U.S.-bound air cargo shipments, we analyzed ACAS data on shipments, risk assessments, and action taken by CBP targeting personnel at the agency's National Targeting Center. Our data analysis was based on a random sample of two percent of all U.S.-bound air cargo shipments from calendar year 2019 provided by CBP, as well as interviews with agency officials. We conducted a site visit to the National Targeting Center, reviewed documentation, and interviewed agency officials to collect information on data management practices and policies. We found the data were sufficiently reliable for our purposes of characterizing the volume of cargo shipments and the risk management steps CBP targeting personnel performed.

[12]GAO, *Aviation Security: TSA Uses a Variety of Methods to Secure U.S.-bound Air Cargo, but Could Do More to Assess their Effectiveness*, GAO-19-162 (Washington, D.C.: Nov. 28, 2018).

To assess the extent to which TSA and CBP have a documented process for ensuring the full exchange of applicable information and data to inform their risk assessment efforts, we reviewed each agency's processes for assessing air cargo security risk. We reviewed relevant TSA and CBP documentation, such as classified and unclassified information, which included aviation threat scenarios and risk (threat, vulnerability, and consequence) ratings for foreign airports. We also interviewed TSA headquarters and CBP National Targeting Center officials who are responsible for collecting and analyzing risk information and developing risk assessments. We assessed TSA and CBP risk assessment processes against recommended practices in DHS's *National Infrastructure Protection Plan* and *Risk Management Fundamentals*.[13]

To assess the extent to which TSA's CT field assessment incorporated key practices for program design and evaluation, we reviewed TSA's planning documentation for the field assessment and interviewed TSA officials about the design and their evaluation of the field assessment. We evaluated TSA's CT field assessment against five key practices established in our guide on designing program evaluations as well as TSA's *Test and Evaluation Guidebook* (T&E Guidebook).[14] We also spoke with a number of officials with experience testing and developing standards for testing CT-based security screening systems including officials at the DHS Transportation Security Laboratory, the National Institute of Standards and Technology, and a former official of the International Electrotechnical Commission.[15]

To identify CBP and TSA's procedures and practices for sharing aviation-related threat information on U.S.-bound cargo, we interviewed CBP and

[13]DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: Dec. 2013), and DHS, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: April 2011).

[14]Transportation Security Administration, *Test and Evaluation Guidebook, Rev. 4* (Washington, D.C.: Dec. 4, 2019). Transportation Security Administration, Assistant Administrator, Office of Security Policy and Industry Engagement, *Requirements for Future Pilots, Projects and Programs*, Memorandum to Division Directors (Aug. 24, 2012); GAO, *Designing Evaluations: 2012 Revision*, GAO-12-208G (Washington, D.C.: Jan. 2012).

[15]The Transportation Security Laboratory is a DHS Federal Laboratory that, among other things, provides TSA with certification and qualification tests and laboratory assessments regarding screening technologies and their ability to detect explosives. It is part of DHS's Science and Technology Directorate, which is the Department's primary research and development arm—it manages science and technology research, from development through transition, for DHS's operational components and first responders.

TSA officials regarding agency procedures and practices for sharing this information with industry stakeholders. For CBP, we interviewed officials, and reviewed related documentation, on the design and functionality of the ACAS program with respect to how ACAS identifies high-risk cargo shipments and communicates with air carriers regarding those shipments. For TSA, we interviewed officials with the agency's Aviation Domain Intelligence Integration and Analysis Cell (ADIAC) within the Intelligence and Analysis office regarding their methods for obtaining and sharing aviation-related threat information from government agencies (including the intelligence community).

The performance audit upon which this report is based was conducted from January 2020 to May 2021 in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We worked with DHS from May to July 2021 to prepare this version of the original Sensitive Security Information report for public release. This public version was also prepared in accordance with these standards.

Background

U.S.-bound Air Cargo and the Air Cargo Supply Chain

Air Cargo is transported into the United States on passenger aircraft (e.g., American and United Airlines), and on all-cargo aircraft (e.g., FedEx, United Parcel Service, and Atlas). U.S-bound air cargo can vary widely in size and include such disparate items as electronic equipment, automobile parts, clothing, medical supplies, fresh produce, and cut flowers. (See figure 1 for examples of palleted air cargo and the cargo-loading process.)

Figure 1: Air Cargo Pallet and Cargo Loaded onto an Aircraft

Source: GAO. | GAO-21-105192

The international air cargo shipping process involves a complex network of business entities that includes individual shippers, manufacturers, transportation companies, freight forwarders, warehouses and air carriers. Entities within the supply chain may provide all services (such as warehousing, consolidation, and loading of air cargo) or only certain services. The standards set by the International Civil Aviation Organization (ICAO) focus on four primary types of entities:[16]

- known individual shippers, manufacturers, other shipping entities (known consignors),[17]
- unknown shippers (unknown consignors, unregulated agents, and other persons),

[16]ICAO is a specialized agency of the United Nations with a primary objective to provide for the safe, orderly, and efficient development of international civil aviation security standards. ICAO member nations (i.e., contracting states) agree to cooperate with other contracting states to meet standardized international aviation security measures, which are detailed in Annex 17 and Annex 14 to the Convention on International Civil Aviation.

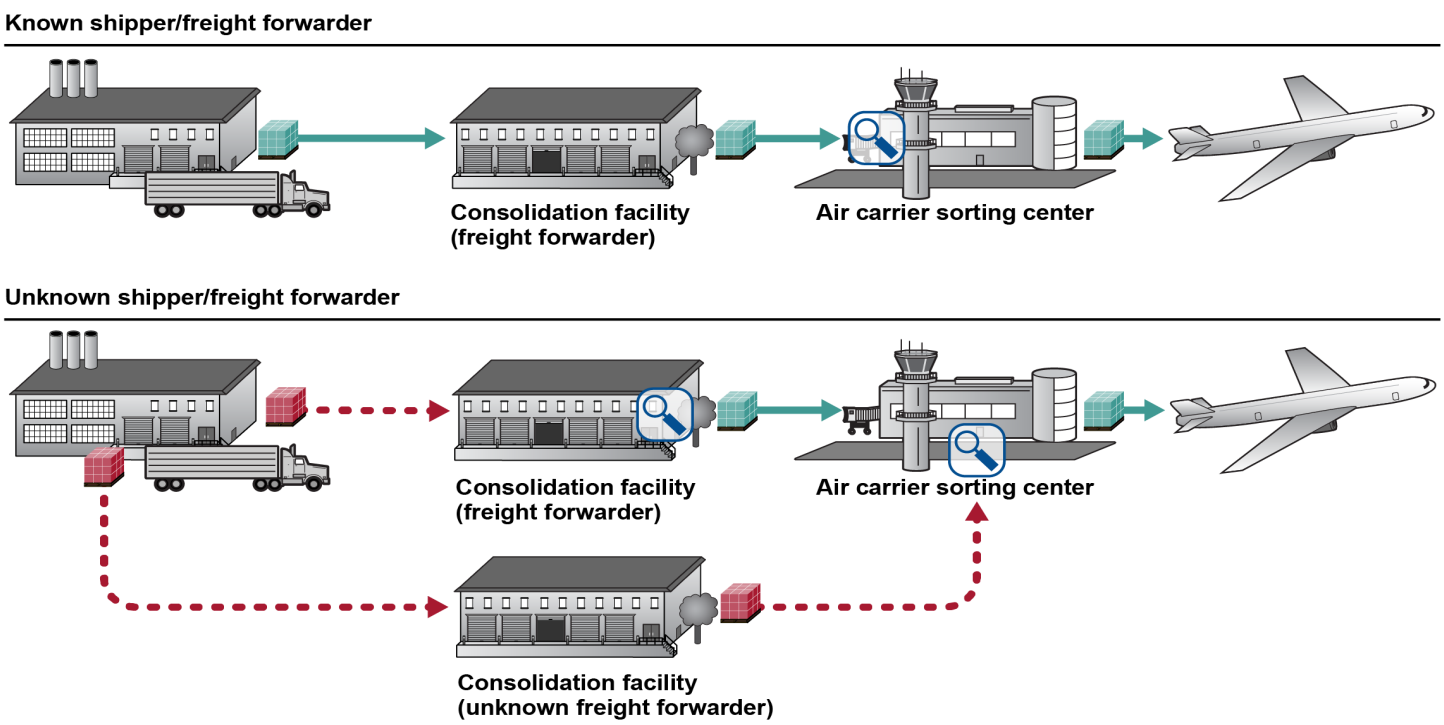
[17]Known individual shippers and manufacturers—referred to as "known consignors"—are those who originate cargo or mail for their own account and whose procedures meet common security rules and standards sufficient to allow the carriage of cargo or mail on any aircraft. According to ICAO, the purpose of the known consignor concept is to place the emphasis for the practical implementation of security controls on the actual shipper or originator of the goods and to ensure the security of air cargo and mail as it moves throughout the supply chain. This requires goods to be produced, packaged, stored, transported, and handled in a manner that ensures their integrity and protects them from unauthorized interference from the point of origin and throughout the secure supply chain.

- freight forwarders, handling agents (regulated agents),[18] and
- commercial air carriers.

Various other air cargo supply chain entities also have responsibilities for applying specific types of security controls in accordance with the international standards. Figure 2 shows an example of the flow of U.S.-bound air cargo and where in the supply chain the cargo can be secured.

[18]A handling agent—known as a "regulated agent"—is a freight forwarder or any other entity that conducts business with an operator and provides security controls that are accepted or required by the appropriate authority in respect of cargo or mail.

Figure 2: Example of the Flow of Air Cargo Transported to the United States from Foreign Airports



Shipper/manufacturer sends air cargo

Known shippers and freight forwarders have an established business relationship with other supply chain entities, such as air carriers, and have applied security measures accepted or required by the appropriate foreign government regulatory authority. Unknown shippers and freight forwarders do not meet these criteria.

Consolidation facility

Shippers may bring air cargo to freight forwarders or unknown freight forwarders, who, before loading cargo onto trucks and delivering it to air carriers' sorting and storage locations, may consolidate shipments from a number of shippers. In addition, freight forwarders screen cargo for security purposes prior to delivering the cargo to air carrier facilities for safe storage until the cargo is loaded onto U.S.-bound flights. Unknown freight forwarders do not screen cargo.

Air carrier sorting center

At an air carrier's sorting center, which is typically located on airport property, either the air carrier or cargo handling agents sort, then screen cargo according to the air carrier's TSA-approved security program.

Secure cargo
Unsecure cargo
Screened/secured

Source: GAO analysis of Transportation Security Administration (TSA) information. | GAO-21-105192

Note: A known shipper may also directly package air cargo and deliver it to an air carrier's sorting center.

To secure cargo, a known consignor is required to produce, package, store, and transport goods in a manner that ensures their integrity and protects them from unauthorized interference from the point of origin. After cargo is secured, subsequent supply chain entities must apply security measures accepted or required by the appropriate national

authority, including measures to ensure the secure transport of cargo. Upon arrival at the air carrier's sorting center, the air carrier or cargo handling agent must verify the known consignor/regulated agent status and that the cargo was transported securely before accepting it.

TSA and Air Carrier Responsibilities for Securing U.S.-bound Air Cargo

The Aviation and Transportation Security Act (ATSA) provides TSA responsibility for securing U.S. and foreign-flagged air carrier operations to, from, within, or overflying the United States, as well as the foreign point-to-point operations of U.S.-flagged carriers.[19] ATSA requires that TSA provide for the screening of all passengers and property, including U.S. mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation.[20] ATSA further requires that a system be in operation to screen, inspect, or otherwise ensure the security of the cargo transported by all-cargo aircraft in air transportation and intrastate air transportation, without establishing a firm deadline for the implementation of such a system.[21]

To help enhance civil aviation security, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), mandated that DHS establish a system by August 2010 to screen 100 percent of air cargo transported on all passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure security of all such passenger

[19]See generally Pub. L. No. 107-71, title I, § 101(a), 115 Stat. 597, 597-602 (2001) (codified, as amended, at 49 U.S.C. § 114); 6 U.S.C. §§ 203 (TSA functions transferred to DHS), 233 (functions of TSA), 234 (preservation of TSA as a distinct entity). For purposes of this report, the term "air carrier" includes the passenger and all-cargo operations of both U.S.-flagged air carriers operating under TSA-approved security programs in accordance with 49 C.F.R. part 1544 and foreign-flagged air carriers operating under security programs deemed acceptable by TSA in accordance with 49 C.F.R. part 1546. For purposes of this report, the security programs of both U.S. and foreign-flagged air carriers are referred to as "TSA-approved security programs."

[20]See Pub. L. No. 107-71, § 110(b), 115 Stat. at 614 (codified, as amended, at 49 U.S.C. § 44901(a)).

[21]See Pub. L. No. 107-71, § 110(b), 115 Stat. at 615 (codified, as amended, at 49 U.S.C. § 44901(f)) (as added by ATSA, subsection (f) required the system to be in operation as soon as practicable after the date of enactment, November 19, 2001; subsection (f) in its current form requires such system to be in operation as soon as practicable without reference to ATSA's date of enactment).

aircraft carrying cargo.[22] TSA reported that it met the mandate to screen 100 percent of domestic air cargo transported on passenger aircraft in August 2010 and U.S.-bound air cargo transported on passenger aircraft from foreign airports in August 2013.[23]

There is no comparable 100 percent screening requirement in statute for cargo transported to the United States on all-cargo air carriers.[24] However, TSA requires that all cargo transported on U.S.-bound flights be screened or subjected to security controls that prevent the introduction of explosives, incendiaries, or other destructive devices.[25] If the cargo comes from known shippers or freight forwarders, TSA's all-cargo security program does not require any additional screening unless the cargo piece exceeds a certain weight. All cargo from unknown shippers or freight forwarders must be screened.

[22]See Pub. L. No. 110-53, title XVI, § 1602(a), 121 Stat. 266, 478 (2007) (codified, as amended, at 49 U.S.C. § 44901(g)(1)) (providing in its current form that "[t]he Secretary of Homeland Security shall establish a system to screen 100 percent of cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure the security of all such passenger aircraft carrying cargo.").

[23]Transportation Security Administration, *Air Cargo Statistics and Certification of 100-Percent Air Cargo Screening: Fiscal Year 2013 Report to Congress* (Washington, D.C.: August 19, 2013).

[24]As of May 2021, domestic and foreign-flagged all-cargo air carriers transporting cargo for U.S. locations (domestically) and non-U.S. locations (outbound) are required to search cargo for "stowaways"—i.e., open and screen all items over 150 pounds (68.0 kg) (with limited exceptions) on every flight to ensure there are no unauthorized individuals present. This screening must be performed after acceptance of the cargo, but prior to loading the cargo onboard the aircraft for the first air leg; or, screen all items over 150 pounds on every flight in accordance with the Carbon Dioxide Monitor Stowaway Detection System Screening Procedures and in accordance with Section 7.2. of the Standard Screening Procedures for Air Cargo for U.S. and non-U.S. locations, to ensure there are no unauthorized individuals present, except as provided in Section 8.5.1.C.). According to a senior TSA official, on June 30, 2021, TSA will require domestic and foreign-flagged all-cargo air carriers to screen 100 percent of outbound cargo transported on all-cargo aircraft. This will not change current U.S. inbound requirements for all-cargo aircraft at this time.

[25]TSA security programs require international inbound cargo transported on all-cargo aircraft to be subjected to a stowaway search or be screened for explosives depending upon the risk attributed to the shipments (e.g., Air Cargo Advance Screening—ACAS—targeting), or the presence of Security Directives/Emergency Amendments at certain locations. If an all-cargo carrier is operating under a NCSP Recognition, it would be required to apply the security measures required by that host country's cargo security program, which may include screening and or application of other security controls.

Air carriers are responsible for implementing TSA security requirements.[26] These requirements include measures related to accepting, handling, and screening cargo; training employees in security and cargo screening procedures; testing employee proficiency in cargo screening; and controlling access to cargo areas and aircraft. If threat information or events indicate that additional security measures are needed to better secure the aviation sector, TSA may issue revised or new security requirements in the form of security directives or emergency amendments when more immediate action on behalf of air carriers is necessary.[27] Air carriers must implement the requirements set forth in applicable security directives or emergency amendments (unless otherwise approved by TSA to implement alternative security measures) in addition to requirements already imposed and enforced by TSA to remain compliant with their respective security programs.

Under TSA regulations, air carriers are responsible for ensuring the security of the air cargo they transport, and TSA requirements specify methods and technologies that may be used to secure U.S-bound air cargo, including screening procedures. Specific screening methods outlined in the 9/11 Commission Act, for example, include X-ray systems, explosives detection systems,[28] explosives trace detection,[29] explosives detection canine teams certified by TSA, and physical search together with manifest verification.[30] The 9/11 Commission Act, however, requires that screening involve a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security. Solely

[26]The security policies, procedures, and systems the air carriers use to comply with the requirements are documented in TSA-approved security programs.

[27]In general, TSA issues security directives to impose such requirements on U.S.-flagged air carriers and emergency amendments to impose such requirements on foreign-flagged air carriers, typically when immediate action is required. See 49 C.F.R. §§ 1544.305, 1546.105(d).

[28]An explosives detection system machine uses computed tomography technology to automatically measure the physical characteristics of objects in baggage. The system automatically triggers an alarm when objects that exhibit the physical characteristics of explosives are detected.

[29]An explosives trace detection machine is used to chemically analyze trace materials after a human operator swabs the item to identify any traces of explosive material.

[30]See Pub. L. No. 110-53, § 1602(a), 121 Stat. at 479 (codified, as amended, at 49 U.S.C. § 44901(g)(4)) (providing further that the TSA Administrator may approve additional methods for ”screening,” which is defined as physical examination or nonintrusive methods of assessing whether cargo poses a threat to transportation security).

performing a review of information about cargo contents or verifying the identity of the cargo's shipper, when not performed in conjunction with the screening methods outlined above, does not meet requirements.

ACAS

TSA and CBP initiated the ACAS pilot in December 2010, in response to the October 2010 printer cartridge plot, to more readily identify high-risk cargo on passenger and all-cargo aircraft departing from foreign airports to the United States. The ACAS pilot operated for more than 7 years and ended on June 12, 2018, with the issuance of the Interim Final Rule, which transitioned the program from a voluntary pilot to a mandatory program for all air carriers transporting commercial cargo from last point-of-departure airports to the United States.[31] CBP instituted an "informed compliance period" during the first year after the pilot (June 12, 2018, to June 12, 2019) delaying penalties to allow air carriers to send data while working out the details of their business process changes to accommodate the requirements of the new program.

In 2001, CBP established the National Targeting Center to conduct risk-based vetting of both passengers and cargo attempting to enter the United States. CBP personnel at the National Targeting Center collect and analyze data on cargo entering the United States and identify high-risk shipments. Air carriers submit cargo manifest data to CBP's ATS prior to loading at all foreign last point-of-departure airports, and CBP uses ATS to review these data to identify high-risk shipments.[32] ATS allows CBP, if warranted, to issue instructions to air carriers to, among other things, provide any additional information that CBP may need on the shipment or perform required screening per the carrier's TSA-

[31]Air Cargo Advance Screening (ACAS), 83 Fed. Reg. 27,380 (June 12, 2018) (codified at 19 C.F.R. pts. 12, 113, 122, 141, 178 & 192). See 19 C.F.R. §§ 122.48 (Air Cargo Manifest), 122.48a (Electronic Information for Air Cargo Required in Advance of Arrival, 122.48b (Air Cargo Advance Screening (ACAS)).

[32]While CBP partnered with TSA in establishing ACAS and TSA personnel are involved in the program, CBP is primarily responsible for administering ACAS out of the agency's National Targeting Center through the use of the ATS.

approved security program before such cargo is loaded onto U.S.-bound aircraft.[33]

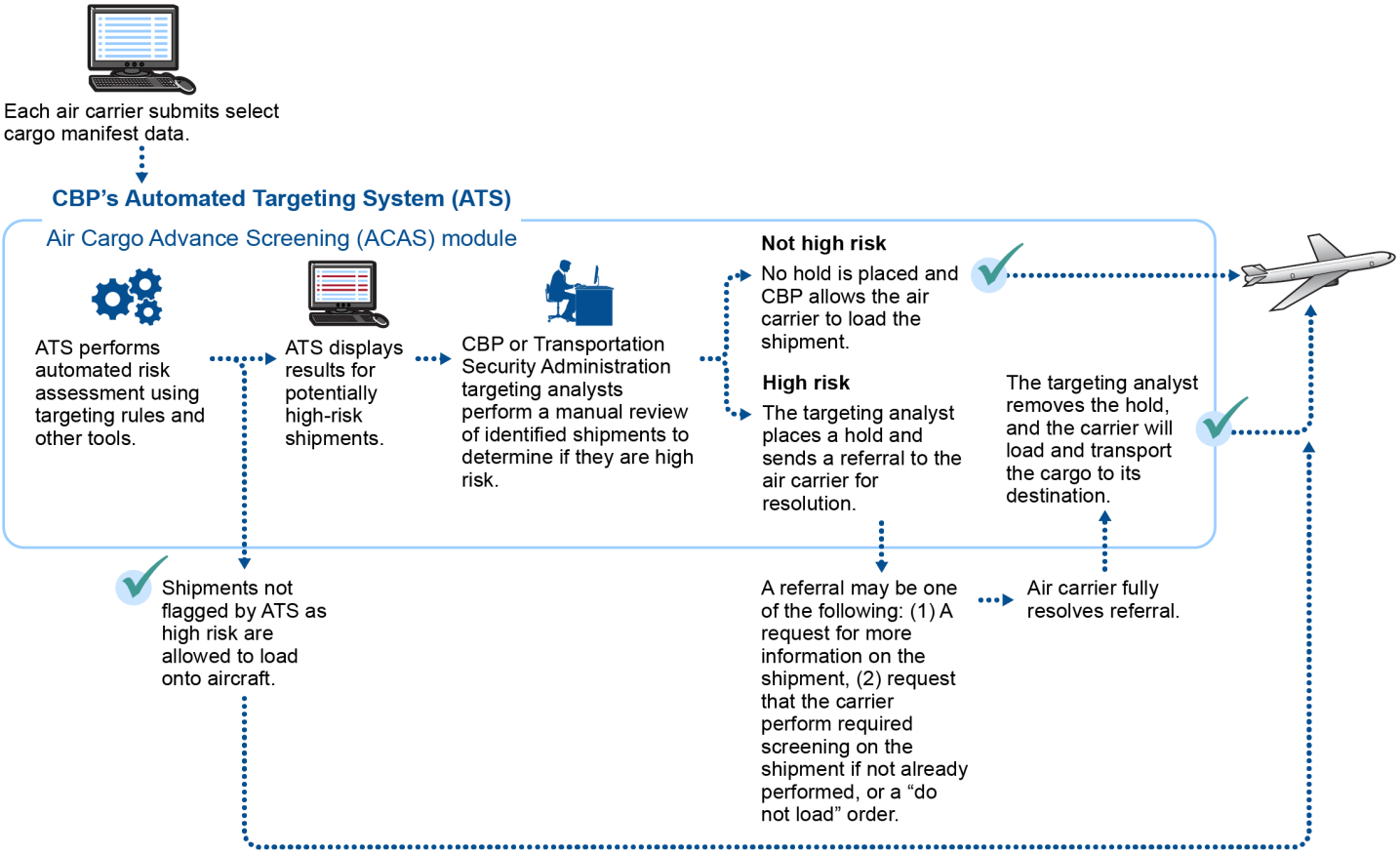
As shown in figure 3, ACAS is a module within CBP's ATS. Once a carrier submits cargo manifest data to CBP, ATS automatically performs a risk assessment using risk-based targeting rules and other tools that evaluate the inbound cargo shipments for chemical, biological, radiological, nuclear, and explosive threats.[34] The ATS displays the results of this automated risk assessment as potentially high-risk cargo shipments for CBP's review. During their manual review of the shipments identified by ATS, CBP or TSA targeting analysts (targeters) at CBP's National Targeting Center research the manifest data against other sources of information, such as law enforcement databases and classified intelligence sources.[35]

[33]TSA officials clarified that in instances when CBP notifies an air carrier that a particular shipment is high risk through ACAS, it is not necessary for the carrier to perform additional screening if it has already performed the TSA-required screening on the shipment. In these instances, the air carrier provides CBP personnel with a statement confirming that enhanced screening was completed on the cargo.

[34]Under ACAS, CBP requires air carriers to provide six data elements for each cargo shipment. These data elements are the air waybill number, shipper name and address, consignee name and address, cargo description, total quantity based on the smallest external packing unit, and the total weight of the cargo. DHS deems the specific risk assessment tools CBP and TSA use to evaluate inbound cargo shipments to be sensitive information and therefore we do not discuss the details of these tools.

[35]After reviewing submitted ACAS and other data, CBP may issue a "do not load" referral to prevent high-risk air cargo that potentially contains a bomb, improvised explosive device, other explosive material, or other risks that may pose a lethal threat to the aircraft, from being loaded.

Figure 3: Air Cargo Advance Screening Process for Addressing High-Risk Air Cargo Transported to the United States from Foreign Airports



Source: GAO analysis of U.S. Customs and Border Protection (CBP) information; Art Explosion (clip art). | GAO-21-105192

TSA's Air Cargo Screening System Field Assessment

TSA's Air Cargo Screening Qualification Test Process

TSA qualifies explosives detection systems for use in screening air cargo through their Air Cargo Screening Qualification Test process, which TSA describes in its February 2020 process guide.[36] Once a system is certified

[36]Transportation Security Administration. Air Cargo Screening Qualification Test Qualification Process Guide (Request for Information 70T04020I9LRCA109) (Arlington, VA: 2020).

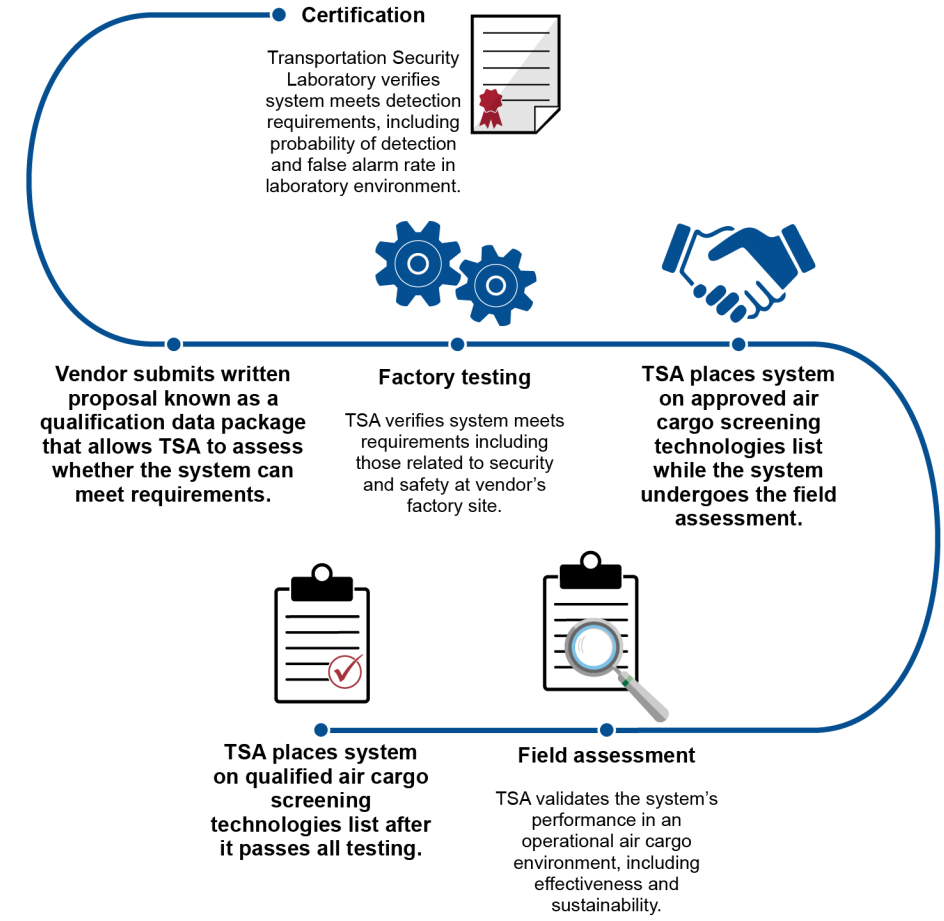
at DHS's Transportation Security Laboratory against TSA threat detection standards, it can enter the air cargo qualification screening process (see fig. 4). Following initial certification, the vendor submits a written proposal, known as a qualification data package, containing information about how the system meets TSA's requirements for air cargo screening.[37] After TSA reviews and accepts the qualification data package, TSA conducts two additional rounds of testing: factory testing and a field assessment. Factory testing consists of TSA's review of vendor-provided data and independent audits of the system at the vendor's factory to verify it meets requirements. After successful factory testing, the system is "approved" by TSA.[38] An "approved" system then undergoes a field assessment where the system must meet all requirements in an air cargo screening environment. Following successful completion of the field assessment, the system is "qualified" by TSA for use.[39]

[37]TSA's process also includes a pre-proposal white paper phase where TSA can provide feedback before the vendor prepares a full qualification data package.

[38]"Approved" systems are conditionally approved by TSA for screening operations and are currently undergoing or scheduled to undergo a field assessment. A system has 36 months from the time it is added to the "approved" section to pass the field assessment.

[39]TSA tracks the "approved" and "qualified" systems on its air cargo screening technology list. Air carriers authorized to screen cargo are required to use an "approved" or "qualified" system from this list, but are encouraged by TSA to use a "qualified" system, since "approved" systems may be removed from the list if they do not pass the field assessment within 36 months.

Figure 4: An Overview of the Transportation Security Administration's (TSA) Air Cargo Screening Qualification Test Process for Explosives Detection Systems



Source: GAO analysis of TSA policy and guidance. | GAO-21-105192

Purpose of Field Assessments

TSA's air cargo screening qualification process follows the principles of the TSA Test and Evaluation Guidebook (T&E Guidebook) for designing and executing a field assessment.[40] The purpose of these assessments, according to the T&E Guidebook, is to independently validate that the system meets TSA's requirements when used in the field. Requirements

[40]Transportation Security Administration, *Test and Evaluation Guidebook, Rev. 4* (Arlington, VA: 2019). The TSA T&E Guidebook refers to this phase of testing as operational testing. For the air cargo qualification process, which is not an acquisition program, TSA refers to this testing phase as a field assessment.

that TSA would typically assess in the field include the system's ability to detect threats (probability of detection), how many alarms it generates from objects without a real threat (false alarm rate), and how often a piece of machinery breaking takes the system offline (reliability, maintainability, and availability). Many of these parameters are first tested in the laboratory environment where TSA can, for example, test the system against a wide range of explosives threats. However, according to the T&E Guidebook, it remains necessary to independently verify that the system still meets key requirements in the field where environmental conditions or the stream of commerce could affect the system's performance.

Overview of TSA's Field Assessment

From January 2020 through April 2021, TSA conducted a field assessment of a CT-based explosives detection system in response to the Act, which directed TSA to conduct a feasibility study and pilot program on the use of CT[41] to screen air cargo.[42] In 2019, TSA published its Computed Tomography Feasibility Study and began a pilot testing program in January 2020 at the United Parcel Service Worldport facility in Louisville, Kentucky.[43] To meet the pilot requirement, TSA officials said that, without supplemental funding for a pilot program, they adapted a previously planned field assessment for the qualification of a CT-based explosives detection system, which this report refers to as the CT field assessment.[44] To conduct this assessment, TSA retrofitted a conveyor belt parcel handling system at the United Parcel Service Worldport Facility with a CT system. Over the course of the field assessment, the

[41]Computed Tomography (CT) is an imaging technology that is widely deployed in the medical industry and has found applications in airport screening to screen checked bags for explosive threats.

[42]Pub. L. No. 115-254, div. K, title I, subtitle B, § 1925 (Computed Tomography Pilot Programs), 132 Stat. at 3563-64.

[43]Transportation Security Administration, *Computed Tomography Feasibility Study.* (Washington, DC: Nov. 18, 2019). The *2019 Computed Tomography Feasibility Study* determined that CT-based explosives detection systems might find some applications for air cargo screening but that widespread adoption was not economically or practically feasible.

[44]TSA classifies systems that image parcels and use an algorithm to determine the presence of explosives as an explosives detection system. An automated detection system is certified as an explosives detection system if it passes certification testing at the Transportation Security Laboratory. An explosives detection system may use CT as the technological approach to detect explosives, but use of CT is not required for a system to qualify as an explosives detection system. For the purposes of this field assessment, TSA was qualifying a CT-based explosives detection system.

CT system inspected 1,000 to 4,000 individual parcels per day, which ranged in contents and size, up to the maximum dimensions of the CT system.[45] TSA officials produced monthly data reports on the results of the field assessment and told us they plan to produce a final report by the end of fiscal year 2021.

Prior Reports on Inbound Air Cargo Security

In 2018, we reported on TSA's progress in assessing and mitigating risks to inbound air cargo.[46] Our analysis of TSA data found that air carriers were in full compliance with cargo security requirements in 84 percent of the nearly 5,000 cargo inspections conducted from fiscal years 2012 through 2017; about 75 percent of foreign air assessments TSA conducted during that timeframe complied with international air cargo standards. We also found that, while TSA had or was developing performance measures to assess the effectiveness of its foreign airport assessment and air carrier inspections programs, these measures did not address cargo-specific vulnerabilities identified during airport assessments. Nor did the measures differentiate efforts to secure air cargo from those for securing passengers in the case of air carrier inspections.

We recommended, among other things, that TSA develop and monitor outcome-based performance measures for determining the effectiveness of the cargo portion of its foreign airport assessments and differentiate the extent to which air carriers correct violations related to cargo for its air carrier inspection program. In October 2019, TSA addressed these recommendations through the implementation of outcome-based performance measures for assessing the effectiveness of the cargo portion of its foreign airport assessment and air carrier inspections.

In May 2020, DHS's Office of Inspector General reported on the extent to which CBP's ACAS program has prevented air carriers from transporting high-risk cargo into the United States.[47] The DHS Office of Inspector General found, among other things, that in fiscal years 2017 and 2018,

[45]According to TSA's requirements, the system shall accept parcels up to at least 39 inches long, 24 inches wide, and 16 inches tall. Transportation Security Administration, Functional Requirements Document: Air Cargo Explosive Detection System (EDS), Version 1.0 (Arlington, VA: March 29, 2019).

[46]GAO-19-162.

[47]Department of Homeland Security, Office of Inspector General, *CBP's ACAS Program Did Not Always Prevent Air Carriers from Transporting High-Risk Cargo into the United States*, OIG-20-34 (Washington, D.C.: May 11, 2020).

CBP did not always prevent air carriers from transporting air cargo shipments deemed high risk into the United States until they had resolved all ACAS referrals, as required by federal regulations.[48] The DHS Office of Inspector General attributed these occurrences to inadequate CBP and TSA policies and procedures that did not ensure air carriers resolved referrals timely or appropriately. It recommended that CBP develop and implement procedures to ensure air carriers resolve ACAS referrals before transporting high-risk cargo to the United States.[49]

DHS Has Multiple Air Cargo Security Programs and Has Taken Steps to Measure Their Effectiveness

TSA and CBP have multiple programs in place for the security of U.S.-bound air cargo. TSA has its air carrier inspection and airport assessment programs for assessing compliance with security requirements and adherence to standards and recommended practices pertaining to air cargo. TSA also has the NCSP Recognition Program, to evaluate the air cargo security programs of foreign countries. Lastly, through its ACAS program, CBP identifies high-risk air cargo shipments. The following is an overview of these various TSA and CBP air cargo security programs and their methods and plans for assessing their effectiveness.

[48]The DHS Office of Inspector General found that out of a random sample of 309 CBP referrals made in fiscal years 2017 and 2018 to air carriers regarding air cargo shipments deemed high-risk, air carriers did not fully resolve 138 (45 percent) before the cargo departed for the United States. During the ACAS pilot period (from 2010 through June 2018), because the pilot was voluntary, not all ACAS pilot data were transmitted in a timely manner and not all ACAS referrals were resolved prior to departure (see 83 Fed. Reg. at 27,387). After the pilot period, CBP established a mandatory ACAS Program requiring any ACAS referral to be resolved prior to departure of the aircraft (see 83 Fed. Reg. at 27,387-27,388).

[49]CBP concurred with this and other DHS Office of Inspector General recommendations. According to DHS's Office of Inspector General, all four recommendations remained open and resolved as of March 2021, meaning CBP has taken steps to satisfy the intent of the recommendations but they remain open until CBP provides documentation to substantiate that all planned corrective actions have been completed.

TSA's Air Carrier Inspection Program: Monitoring Compliance with Air Cargo Security Requirements

Screening of Individuals on All-Cargo Flights

According to the Transportation Security Administration (TSA), as of January 2021, security requirements for all-cargo air carriers allow a pilot to designate any authorized individual traveling on an all-cargo flight as a "crewmember" for that flight. These individuals are then subject to the same screening requirements for that flight as the air crew (pilot, co-pilot, and navigator). TSA officials stated that all-cargo air carriers have historically used this option so that such individuals do not have to undergo the screening required for non-crewmembers, which is an identification check and a search of their person and accessible property (comparable to passenger screening for commercial flights).

In contrast, TSA requires that crewmembers undergo an identification check, but not a search or screening of accessible property. According to TSA, authorized individuals might include air carrier personnel or payload (cargo) specialists, such as handlers responsible for live animals. TSA stated that, as of March 2021, they were in the process of updating all air carrier security requirements, to include a clarified definition of "crewmember" and other requirements, such as requisite training. TSA expects to complete the updates by September or October 2021.

Source: TSA. | GAO-21-105192

TSA monitors the extent to which air carriers comply with the various sets of cargo-related security requirements for flights from foreign locations to the U.S. through its air carrier inspection program.[50] During the course of our 2018 work on U.S.-bound air cargo, we learned that TSA was tracking a newly developed performance measure on the percentage of inspection findings that have been closed based on the air carrier successfully addressing the deficiency identified by the TSA inspectors.[51] TSA began monitoring and reporting internally on this measure in the third quarter of fiscal year 2019. However, TSA was tracking the status of all violations the inspectors identified during the air carrier inspections, not just those related to cargo.

As a result of our 2018 recommendation, TSA now breaks out the results for air cargo among the inspection findings by way of a technology tool that separately tracks the different categories of violations identified, including cargo.[52] TSA officials stated that they, through use of the technology tool, review the results for these separate categories on a weekly basis. For the period of July 1, 2019 (when TSA began using the technology tool to track cargo findings identified in air carrier inspections) through August 31, 2020, TSA identified a total of 29 cargo-related findings as a result of its inspections of air carriers transporting cargo from foreign airports to the United States. As of August 31, 2020, TSA had resolved all 29 findings with counseling or a warning notice and closed them accordingly.

As of January 2021, TSA was working to expand performance measurement regarding adherence to air cargo security requirements that would move beyond measuring the level of air carriers' compliance with the requirements. These efforts would potentially result in additional measures to assess the overall effectiveness of the various air cargo security requirements in preventing threats to air cargo security. Specifically, according to officials, TSA is working toward using air cargo covert testing at foreign airports as a potential proxy outcome measure for

[50]TSA refers to the collective security requirements that apply to each class of air carrier as "standard security programs" or "security programs." These are the basic requirements that each of the four types of air carriers—domestic and foreign-flagged passenger carriers that carry air cargo and domestic and foreign-flagged all-cargo carriers—must follow. Requirements include those related to cargo acceptance, control and custody of cargo, and screening procedures. For more information on TSA's various cargo security requirements and programs, see appendix II.

[51]GAO-19-162.

[52]GAO-19-162.

assessing the effectiveness of security requirements in preventing threats on flights to the United States. As of December 2020, TSA's Inspection Office was conducting initial outreach to six countries to initiate joint covert testing efforts. Inspection officials added that this effort to engage with the other countries was ongoing and also included joint pilot testing of passenger screening operations with the six countries. TSA's Inspection Office is continuing to negotiate with these and other countries to conduct joint testing at overseas locations. Inspection officials stated that initial efforts are to focus on passenger-oriented covert testing to possibly be followed later by covert testing of cargo.[53]

TSA Airport Assessment Program: Determining the Effectiveness of Security Measures at Foreign Airports

As required by statute, TSA also assesses the effectiveness of security measures (including those related to cargo) at foreign airports using select ICAO standards and recommended practices.[54]

In response to a 2018 recommendation we made on measuring the effectiveness of TSA's airport assessment program, TSA began tracking in July 2019 performance measures specific to the percentage of identified vulnerabilities that have been closed.[55] For this internal reporting, TSA tracked the status of all vulnerabilities inspectors identified during the assessments—regardless of whether they were specific to cargo or other aspects of the airport's operations examined by TSA. To address this recommendation, TSA developed a reporting tool to separately track the different categories of vulnerabilities identified, including air cargo. TSA officials stated they use the reporting tool to review the results for these separate categories on a weekly basis.

For the period of July 1, 2019 (when TSA began using the reporting tool to track cargo vulnerabilities identified in foreign airport assessments) through August 31, 2020, TSA identified air cargo-related vulnerabilities as a result of its foreign airport assessments conducted worldwide during

[53]TSA officials clarified that they are not certain whether TSA will be able to eventually include covert testing of cargo in their joint efforts. Officials attributed this to the early stage of negotiations with other countries regarding joint covert testing. However, TSA's intent is to include covert cargo testing, if possible, following the establishment of the joint passenger-oriented covert testing in these countries.

[54]See 49 U.S.C. § 44907. TSA assesses foreign airports (1) served by a U.S. air carrier, (2) from which a foreign air carrier operates U.S.-bound flights, and (3) that pose a high risk of introducing danger to international air travel; as well as other foreign airports the Secretary of Homeland Security considers appropriate. See id. § 44907(a).

[55]GAO-19-162.

this time period.[56] As of February 2021, 29 of the air-cargo related vulnerabilities remained open. TSA identified other vulnerabilities, in addition to those related to air cargo security, during this time period, including vulnerabilities related to access control and passenger and baggage screening vulnerabilities.

TSA's NCSP Recognition Program: Assessing Foreign Countries' Air Cargo Security Programs

TSA developed the NCSP Recognition Program to compare and assess foreign air cargo security programs and standards and determine if those programs provide a level of security that is commensurate with TSA's standards for U.S.-bound air cargo shipments. If so, TSA may recognize the country as part of the NCSP Recognition Program and allow air carriers to follow the foreign country's security program instead of following their individual TSA-approved security program. Air carriers must follow the foreign country's security program even if it imposes security requirements over and above what TSA requires.

In response to a 2018 recommendation we made that TSA develop measures for assessing the effectiveness of the NCSP Recognition Program, TSA developed performance measures specific to the NCSP, and in October 2019 began tracking them.[57] These include (1) the number of TSA's recommendations implemented by foreign countries seeking approval of their air cargo security programs under the NCSP Recognition Program and (2) the number of onsite validations to assess program implementation. In March 2021, TSA issued its performance report for the fourth quarter of fiscal year 2020, which provided information on the status of key activities TSA links to outcomes for the NCSP Recognition Program.[58] The report noted that many of the planned program activities during the year had to be postponed or canceled due to the ramifications of the COVID-19 pandemic. According to the report, TSA is reviewing and revising its plans for fiscal year 2021 to accommodate and mitigate these challenges.

[56]DHS deems air cargo and other types of security-related vulnerabilities identified through TSA foreign airport assessments to be sensitive information. Therefore, we have omitted (1) the number of air cargo security-related vulnerabilities TSA identified, (2) the number of air cargo security-related vulnerabilities closed, and (3) the number of access control and passenger and baggage screening security vulnerabilities identified.

[57]GAO-19-162.

[58]Transportation Security Administration, Recognition, Policy, and Programs Section, *NCSP/K9SP Recognition Programs Quarterly Performance Report*, *July-September 2020*.

CBP's ACAS Program: Identifying High-Risk Cargo

According to the Interim Final Rule establishing ACAS as a mandatory program, the intent of ACAS is to identify high-risk cargo before it departs a foreign airport for the United States. This identification process begins once the air carrier provides mandatory data on the cargo shipment to CBP's ATS—such as a description of cargo and the name and address of the shipper. CBP and TSA require the data to be provided before the cargo is loaded onto the aircraft. See appendix II for summary data including the number of shipments for which CBP received required data, number of reviews performed on those data, and resulting referrals to air carriers based on those reviews.

CBP officials utilize manual queries and reports, on an as-needed basis, to monitor the level of air carrier compliance with ACAS reporting and referral requirements.[59] CBP officials stated CBP is developing an information technology tool—the ACAS Dashboard—to improve its ability to monitor air carriers' compliance with ACAS requirements. The officials explained that this tool would automatically identify air carriers' potential compliance issues and enhance their ability to monitor ACAS compliance. The officials added that they expect this tool to be used in conjunction with the manual queries and reports to assess compliance with ACAS requirements.[60]

CBP officials said they plan to assess the effectiveness of the ACAS program by using Dashboard data to determine the extent to which air carriers submit required data to ACAS and the extent to which cargo identified as high risk is cleared for shipment. According to these officials, Dashboard development is ongoing and their priority is to complete its development to enable them to monitor air carriers' compliance. As of November 2020, the agency was in the process of determining the exact data to be included on the Dashboard and finalizing its format.

[59]Based on CBP's compliance reviews of ACAS submissions and referral data conducted prior to starting development of the ACAS Dashboard in late calendar year 2020, CBP officials said their personnel have made phone calls, sent emails, and (in some cases) sent warning letters to air carriers for missing or untimely ACAS data submissions.

[60]Based on our review of the present version of the ACAS Dashboard, it automatically collects and presents information on air carriers' compliance with required ACAS data submissions and referrals. CBP officials expect that the Dashboard will enable them to more easily see the number of instances—out of the total data on each shipment required by CBP—where an air carrier may have failed to provide required data. CBP personnel are to also review and monitor information on the Dashboard on the status of ACAS referrals to determine whether the referrals are finalized in a timely manner.

CBP Uses ACAS to Identify High-Risk Air Cargo Shipments

ACAS Uses Risk-Based Targeting Rules and Other Tools to Identify High-Risk Cargo Shipments

ACAS program documentation shows that, as part of the ATS targeting efforts, CBP identifies high-risk shipments by applying risk assessment tools, such as applying sets of "targeting rules," to compare industry information on U.S.-bound air cargo against potential threats and other risk factors.[61] CBP personnel can create ACAS targeting rules for multiple purposes, some of which are not directed at counter terrorism and instead focus on various compliance and regulatory issues that CBP is concerned with, but fall outside of aviation security.[62]

With regard to the number of shipments that ACAS identified for review, we obtained a sample of ACAS shipment data from CBP for the period January 1, 2019, through December 31, 2019.[63] Based on our analysis of this calendar year 2019 ACAS data sample, we estimate that ATS identified 0.42 percent of all shipments during this timeframe for manual review. Further, we estimate that

- 0.04 percent were associated with at least one type of risk assessment tool,
- 0.04 percent were associated with at least one targeting rule, and

[61]Because DHS has designated the risk assessment tools and procedures CBP and TSA use to assess inbound air cargo shipments as sensitive information, we have omitted specific details about these tools.

[62]According to CBP officials, these other ACAS targeting rules will result in a notification to specified individuals in CBP who are monitoring these issues. Specific examples of these other targeting rules include anti-smuggling and trade enforcement concerns, in addition to rules for tracking and trend analysis, where the rules culminate in a notification to specified individuals.

[63]Our data analysis is based on a random sample provided by CBP of 3,280,716 shipments, 2 percent of all U.S.-bound air cargo shipments during calendar year 2019. All estimates have 95 percent confidence intervals of +/- 0.007 percent or less, unless otherwise noted.

- 0.27 percent of all shipments during this time period identified in ATS for manual review were not associated with an active targeting rule or other type of risk assessment tool.[64]

According to CBP officials, situations related to the shipments falling within the 0.27 percent above could arise, for example, when ATS identifies a shipment based on missing information. When the air carrier provides or updates the missing information, this response causes ATS to cease highlighting that shipment given that the missing information was provided. However, because the shipment is already identified in ATS for manual review due to the original missing information, it remains highlighted until an ACAS targeter reviews and clears it.

According to ACAS program documentation, CBP's review of an identified shipment can result in a hold on the shipment and a referral to the air carrier. The referral may direct the air carrier to provide additional information to remedy a data quality issue, conduct a screening, or not load the shipment onto the aircraft (i.e., a "do not load" order). We estimate that CBP placed a hold on 0.001 percent of all calendar year 2019 shipments after being identified by ATS for manual review.[65] CBP officials stated that other escalatory actions are possible apart from cargo holds. For example, for a small subset of shipments, targeters perform carrier outreach and "informed compliance" through industry outreach (emails, phone calls, conference calls) as well as warning letters about non-compliance that could result in penalties if not corrected.[66]

CBP Periodically Reviews Targeting Rules for Effectiveness

According to CBP officials, CBP routinely reviews targeting rules and other risk assessment tools for effectiveness in identifying shipments of interest and removes or updates those that are out of date or not aligned with the current threat environment. According to these officials, a change in the perceived threat from an entity or target, or an update to laws or regulations, for example, could result in CBP deeming that a rule is no longer necessary. Further, CBP assesses other risk assessment tools for continued relevance based on regular discussions that consider referral

[64]Because DHS has determined that our estimate of the percent of shipments in our sample associated with specific types of risk assessment tools to be sensitive information, we have omitted that percent.

[65]The 95 percent confidence interval for this estimate is +/- 0.00027 percent.

[66]CBP officials generally refer to "informed compliance" as efforts they undertake, short of issuing penalties, to inform air carriers of errors or omissions in required ACAS data submissions.

rate, cargo examination results, and continued relevance to the current threat environment, including intelligence assessments. Officials said the majority of targeting rules are automatically flagged for review and possible expiration on a recurring basis.[67] Additionally, CBP reviews each targeting rule prior to its expiration through a panel review process to determine if it warrants extension, modification, or deactivation. This panel review process involves ACAS stakeholders, including Watch Commanders, Chief Watch Commanders, program managers, and Intelligence Research Specialists.

According to CBP officials, some factors the agency uses to determine whether a targeting rule should be kept active include referral rate to air carriers for further screening, the need for additional information or other instructions, the results of the referrals, and the status of the threat related to the targeting rule. For example, CBP can modify a rule deemed too vague or broad, resulting in too many shipments being identified in ATS, to be more specific. CBP officials added that they do not believe systematic statistical analysis of ACAS targeting rules against performance indicators or other benchmarks (which could be applied to evaluate whether a targeting rule should be kept active) is possible given the unique circumstances around each rule.

According to CBP officials, the efficiency of the ACAS targeting process evolved from fiscal year 2018 through fiscal year 2020. Specifically, CBP focused on refining targeting rules to more efficiently identify potentially high-risk shipments and limit the instances in which lower-risk shipments were identified by ATS for manual review. According to officials, the majority of all air cargo shipments coming through ACAS are from known, high-volume shippers. However, these shipments sometimes have non-security issues such as missing optional data elements.[68]

According to the officials, this refined targeting process is more efficient because it does not require CBP targeters to invest time in researching lower-risk shipments and instead allows them to focus their efforts on shipments that are greater risk. Prior to these refinements, CBP targeters

[67]DHS has determined the review cycle for the targeting rules to be sensitive information, therefore we have generalized the time frames under which the rules are reviewed.

[68]Because DHS has deemed the identification of specific elements to be sensitive information, we characterize these broadly as “data elements.”

checked all shipments associated with triggered targeting rules.[69] Also, according to the officials, collaborating with other U.S. agencies is fundamental to their efforts to improve targeting. In this regard, they noted that the agency has formalized and improved its relationship with the intelligence community to enhance the flow of relevant information that has contributed to these targeting improvements.

TSA and CBP Share Information, but Do Not Have a Documented Process to Ensure the Full Exchange of Data

TSA and CBP have separate procedures for assessing risk for inbound air cargo and share information to inform their respective risk assessments; however, they do not have a documented process that ensures the full exchange of relevant risk data. Officials from both agencies told us they share relevant threat information, but also stated that ACAS trend data, while provided to TSA's Intelligence and Analysis office, is not provided directly to TSA's International Risk Branch, which is responsible for assessing air cargo security risk. A senior TSA International Risk Branch official said they would benefit from receiving ACAS trend data as a potential input to the agency's air cargo risk assessment.

According to the *National Infrastructure Protection Plan*, neither public nor private sector entities can fully understand risk without the integration of wide-ranging knowledge and analysis.[70] DHS's *Risk Management Fundamentals* states that risk management efforts should be coordinated and integrated among all partners with shared or overlapping risk management responsibilities.[71] It also notes that most homeland security measures involve representatives of different organizations and that it is important to have unity of effort among those charged with managing risk to ensure consistent approaches and a shared perspective. Further, an organization must be able to view risk on a comprehensive, enterprise-wide basis—most risk information is viewed by the individuals responsible for managing particular risks, who are not necessarily able to see how risks can affect other parts of the organization or to see the cumulative risks the organization faces.

[69]Due to DHS's determination that details of the process are sensitive, we have omitted them.

[70]DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: Dec. 2013).

[71]DHS, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: April 2011).

TSA, which has primary responsibility for assessing risk from U.S.-bound air cargo, has identified improvised explosive devices planted on aircraft by international terrorists as a significant risk to air cargo security.[72] TSA International Risk Branch officials told us they holistically assess the risk of improvised explosive devices to inbound air cargo security through various mechanisms, including assessment of foreign airports that serve as a last point-of-departure for U.S.-bound cargo, air carrier compliance with U.S. screening regulations, and risk-based threat scenarios. CBP officials told us they also assess risk to inbound air cargo but at the individual-shipment level, through the ACAS program.

According to TSA officials, TSA provides air cargo risk information, such as threat intelligence, to CBP's National Targeting Center analysts, and in the past has also provided risk assessments of foreign airports. A senior official with TSA's International Risk Branch stated that CBP's National Targeting Center, in turn, provides TSA with information on air carriers that do not comply with ACAS requirements. TSA uses this information to inform its air carrier inspections, which feeds into assessments of air cargo risk.[73]

However, CBP officials stated that the National Targeting Center also compiles ACAS shipment data at an aggregate level to assess risk to air cargo security at both the classified and unclassified levels. CBP's National Targeting Center officials said that while they share these trend data as intelligence with TSA's Intelligence and Analysis office, they do not directly share the classified and unclassified ACAS trend data with TSA's International Risk Branch, which is responsible for assessing inbound air cargo risk for TSA. CBP's National Targeting Center officials told us that their primary focus has been on coordinating intelligence information with TSA's Intelligence and Analysis Division and they were not aware that the ACAS trend data were not reaching TSA's International Risk Branch.

TSA and CBP officials said they do not have a documented process that ensures applicable risk assessment information for air cargo security is

[72]According to TSA, the presence of cargo shipments on passenger aircraft increases the security risk level of inbound air cargo. TSA analysis states that together, the risk from inbound commercial passenger aircraft carrying cargo, combined with risk from inbound all-cargo flights, represents approximately 33 percent of the overall risk from international aviation.

[73]According to National Targeting Center officials, they share information with TSA on air carriers that do not comply with ACAS requirements through a shared data platform.

made available to relevant officials. A senior TSA official told us that including ACAS trend data in their overall assessment of inbound air cargo risks could help them ensure a more accurate holistic assessment of risk.

Although CBP shares ACAS information with TSA's International Risk Branch, it does not share ACAS trend data on the millions of air cargo shipments entering the United States each year. As a result, TSA officials responsible for assessing risk to inbound air cargo do not have a complete understanding of the risk posed by inbound air cargo. A documented process that ensures all relevant TSA and CBP offices are informed of and have access to ACAS trend data and other applicable risk data would help assure DHS that it has a comprehensive understanding of risks related to inbound air cargo and allow it to make more informed decisions about how to best mitigate those risks.

TSA's Field Assessment Is Unable to Ensure that the Screening System Meets Detection Standards

We analyzed TSA's CT field assessment against five key design and evaluation practices based on our guidance for program design and evaluation and TSA's test and evaluation guidance.[74] We found that TSA did not fully meet three of the five key practices. TSA incorporated key practices of (1) clarifying program goals and (2) developing evaluation questions. However, TSA partially incorporated the other key practices of (3) selecting an appropriate design approach, (4) collecting all relevant data, and (5) analyzing that data in a way that allows them to draw valid conclusions from the CT field assessment. Because TSA officials did not fully incorporate these key practices, they are unable to ensure that the CT system meets detection standards in the field.

TSA Developed Goals and Key Metrics for Its Field Assessment

TSA identified goals for its CT field assessment and established key metrics related to those goals, in accordance with key design and evaluation practices.[75] TSA's qualification process identified four goals for the CT system to screen air cargo: detection, security, sustainment, and safety. For each goal, TSA developed a relevant evaluative framework and associated metrics. TSA also identified specific goals for the field assessment to evaluate the CT system's operational effectiveness and

[74]The five key practices are: 1) Clarify understanding of the program's goals and strategy; 2) Develop relevant and useful evaluation questions; 3) Select an appropriate evaluation approach for each evaluation question; 4) Identify data sources and collection procedures to obtain relevant, credible information; 5) Develop plans to analyze the data in ways that allow valid conclusions to be drawn from the evaluation questions. For more details on the development of these key practices, see appendix I.

[75]GAO-12-208G.

sustainability. Additionally, TSA established metrics for the field assessment-specific goals, including

- clearance rates through different levels of screening (automated image review, manual image review by screener, and physical search by screener);
- number of parcels screened per hour (throughput); and
- frequency in which the system is available for use between regular maintenance actions and any failures (as measured in terms of reliability, availability, and maintainability).

TSA Developed High-Level Evaluation Questions that Met the Needs of the Field Assessment

TSA developed evaluation questions for each goal of their qualification process. According to key design and evaluation practices, a program should develop relevant evaluation questions that help focus the evaluation on key issues about a program's performance. For their qualification process of the CT system, TSA officials identified an evaluation question for each of their goals: Detection, Security, Sustainment, and Safety. For the specific goals that TSA developed for the field assessment portion of the qualification—Operational Effectiveness and Sustainment—TSA did not identify evaluation questions. However, the high-level evaluation questions they did develop sufficiently achieved the desired effect of identifying key issues about the program's performance, as indicated by the key practice.

TSA Did Not Select an Appropriate Evaluation Approach or Collect All Necessary Data to Fully Assess the Screening System's Operational Effectiveness

TSA did not select an evaluation approach that included collecting necessary data about the CT system's probability of detection in the field as part of its field assessment. According to key design and evaluation practices, a program should select an appropriate evaluation approach and identify ways to collect relevant and credible data.[76] A TSA official told us that they follow the TSA T&E Guidebook in designing their field assessments for air cargo screening technologies, which details how components should plan and execute a test and evaluation strategy. To assess operational effectiveness, the TSA T&E Guidebook states that the test team should gather data on probability of detection, false alarm rate, and throughput in the operational environment. The T&E Guidebook also states that testing officials should identify any testing limitations, and develop and document suitable alternative test methodologies to collect key data when limitations exist.

[76]GAO-12-208G.

According to the TSA's CT field assessment data collection summaries, TSA collected data on packages screened per hour and clearance rates.[77] However, TSA told us they did not measure probability of detection during their field assessment due to the operational difficulties of using live explosives in the field. According to officials, TSA relied on image quality testing as an alternative to directly performing explosives testing during the field assessment.

Officials familiar with the development of the national and international standards for image quality testing of CT systems confirmed that image quality testing could be used to check the CT system's performance in the field. Specifically, representatives at the Transportation Security Laboratory and the National Institute of Standards and Technology said they developed a national standard for image quality testing of CT systems[78] in part to verify that the probability of detection of a CT system in the field matched the tests performed during certification in the laboratory, without using explosives. That said, they noted that the group conducting the test must establish clear traceability—or linkage—back to the laboratory tests conducted with live explosives. This traceability would include confirming that the image quality tests closely correlate with the system's ability to detect threats; capture possible ways the system performance could degrade; and establish, with quantitative metrics, acceptable ranges of the system's performance.

In its field assessment, TSA used a manufacturer-developed operational test kit that automatically performs two of eight image tests from the national standard for image quality testing. However, TSA did not provide independent validation that the operational test kit's results correlated with the system's ability to detect threats and accurately capture ways in which the system's performance could degrade. Furthermore, the

[77]TSA identifies three levels of screening: L1, L2, and L3. L1 corresponds to clearance using only the machine algorithm, L2 is a clearance where an operator views an image of the bag, and L3 is when a parcel is opened for physical inspection.

[78]Institute of Electrical and Electronics Engineers Standards Association, *American National Standard for Evaluating the Image Quality of X-ray Computed Tomography (CT) Security-Screening Systems*. (New York, NY: May 23, 2011). This standard is developed by a working group of the Accredited Standards Committee on Radiation Instrumentation, N42. According to an official at the National Institute of Standards and Technology, the Institute facilitated the development of this standard.

operational test kit provides only a qualitative indicator (green, yellow, or red light) and TSA did not collect any of the underlying quantitative data.[79]

TSA officials said they did not independently validate the test kit used during the CT field assessment or collect the underlying data. They said they did not take these steps because the tests used by the operational test kit and the ranges of acceptable results are established by the manufacturer, and the Transportation Security Laboratory certifies the performance of the operational test kit during laboratory testing. Therefore, TSA officials believe the manufacturer-developed operational test kit provided a sufficient alternative to testing the CT system's probability of detection in the field. However, officials at the Transportation Security Laboratory stated that they do not evaluate or certify the performance of operational test kits for explosive detection systems, and since each manufacturer develops its own kit, the performance of each kit can vary across manufacturers in its ability to detect deterioration in a CT system's performance.

Thus, TSA has not provided its own validation that the test kit traces back to the laboratory tests with live explosives and thus constitutes an acceptable alternative test method to determine the CT system's probability of detection in the field. Without directly verifying the probability of detection in the field or using an independently validated alternative testing approach to determine the probability of detection, TSA will not have an evaluation approach that includes collecting all relevant data to assess whether the CT system meets TSA's requirements. Knowing whether the system meets TSA requirements is essential to TSA when assessing whether to designate a system as "qualified" on its air cargo screening technology list, which determines whether air carriers can use the system to screen cargo.

[79]At the conclusion of our review, TSA officials indicated they were pursuing additional steps to assess the operational test kit by collecting additional data but did not provide any substantiating documentation that this additional information would include quantitative data measured by the test kit.

TSA's Analysis of the Screening System's Performance Data Did Not Include All the Analysis Necessary to Support Its Conclusions

TSA calculated values for the metrics it used to assess the CT system's sustainability and operational effectiveness, but it did not conduct the statistical analysis or, in some cases, set performance thresholds, necessary to determine whether the system meets requirements. According to key practices, a program evaluation should develop plans to analyze performance data to draw valid conclusions about the program.[80] The TSA T&E Guidebook, which TSA officials say they follow in developing all their field assessments for air cargo screening technologies, states that the evaluation should express the statistical confidence with which the test results meet each requirement.[81] Statistical confidence is a mathematical framework that compares a measured value and the error in that measured value against a specified performance threshold to determine, with a certain probability, whether the result meets a requirement.[82] TSA's CT field assessment included the following data and analyses:

Sustainability. According to TSA's project plan, to assess the sustainability of the CT system, TSA was to evaluate reliability, maintainability, and availability by measuring specific metrics: Mean Time between Critical Failures, Mean Time to Repair, Mean Time between Maintenance Activities, and Inherent Availability. TSA was then to compare them to the corresponding performance thresholds. In its August 2020 CT data analysis report, TSA stated that the system met all the required thresholds, but TSA did not perform a statistical analysis to determine the confidence with which the system met those requirements.

Operational Effectiveness. To assess the operational effectiveness of the CT system, according to their CT field assessment project plan, TSA was to measure the rate that the system clears or rejects packages at various levels of screening (automated image review, manual image review by screener, and physical search by screener), including information about the false alarm rate. However, the project plan does not provide performance thresholds that a statistical analysis could compare

[80]GAO-12-208G.

[81]The T&E Guidebook lays out four evaluation categories: "requirement demonstrated with statistical confidence," "requirement demonstrated without statistical confidence," "requirement not demonstrated with statistical confidence," and "requirement not demonstrated without statistical confidence."

[82]The error of a measured value, also known as uncertainty, reflects that no scientific measurement can be made with perfect accuracy. Errors can arise from the measurement instrument or technique, regardless of the care taken to make a measurement.

against.[83] Instead, the CT data analysis report stated that the measured rejection rates were "within expectations and consistent with airport checked baggage screening performance."

However, TSA officials told us that this comparison is limited because checked baggage and air cargo have different operational environments. TSA officials further stated that, although they saw variations between one-half to twice the required false alarm rate in their CT field testing, these variations do not represent a significant deviation, and alarm rates are consistent with the CT systems used for checked baggage screening. Furthermore, TSA officials said they did not set performance thresholds for these metrics because they expect false alarms to vary in the field and every operational environment will be different. However, TSA did not perform additional analysis, such as a Receiver Operating Characteristic (ROC)—which analyzes the tradeoff in a system between probability of detection and false alarm rate.[84] Such an analysis would help TSA understand the impact of the observed deviations in false alarms on the system's performance and whether the system is still meeting requirements with statistical confidence.

TSA officials stated that they plan to include more detailed analysis of the data collected on sustainability and operational effectiveness in their final report, which they expect to produce by the end of fiscal year 2021. However, at the time of our review and despite multiple requests, TSA was unable to provide us with a data analysis plan, final report template, or other documentation that would provide verification that its final report would include an analysis that allows it to establish statistical confidence for each metric, consistent with guidance from the T&E Guidebook. Furthermore, a TSA official said TSA will provide a statistical confidence determination only for those metrics for which it has already defined a confidence interval, which does not include any of the metrics under evaluation in the field assessment.

Without a statistical analysis that considers measurement errors and performance thresholds, and an analysis to evaluate CT system field

[83]Without a performance threshold, the statistical confidence of whether the data meet the requirement cannot be assessed because statistical confidence compares the measured data, and its measured error, with a target value.

[84]See appendix III for a detailed description of ROC analysis. ROC is an example of one analytical tool TSA could use to obtain additional information about probability of detection and false alarm rate, but TSA could identify and use other analytic or experimental methods to obtain this information.

assessment data against those thresholds with statistical confidence, TSA will not be able to determine the extent to which the system is meeting requirements. TSA needs to know whether the system meets requirements to determine whether to designate it as "qualified" on its air cargo screening technology list, which determines whether air carriers can use the system to screen cargo.

CBP and TSA Take Various Steps to Share Threat Information with Stakeholders

CBP Shares Information with Air Carriers through ACAS

CBP shares information with air carriers through ACAS, which, as previously discussed, requires air carriers to submit shipment data on U.S.-bound air cargo prior to departure from last point-of-departure airports. ACAS serves as an information-sharing mechanism because it allows CBP to communicate potential cargo security concerns directly with air carriers.

CBP communicates these concerns to the air carriers by way of referrals for additional information or screening on the shipment. Seven of the 11 air carriers we communicated with stated that it would be beneficial for them to receive additional information on the reasons why CBP had decided to make the referral. CBP officials acknowledged that they were limited in what they could provide when information supporting the referrals was law enforcement sensitive or classified intelligence. However, the officials told us that they include as much information as possible in the referrals when they send them to the air carriers.

TSA Program to Share Aviation Threat Information with Stakeholders

In response to recommendations we made in 2014 for TSA to strengthen information sharing with transportation stakeholders and ensure that stakeholders receive security-related information in a timely manner, TSA developed the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC), which operates within TSA's Intelligence & Analysis Division.[85] According to TSA, ADIAC is designed to function as a clearinghouse and repository for aviation-related threat information and intelligence from

[85]GAO-14-506.

government agencies (including the intelligence community) and the aviation industry for U.S.-bound air cargo.[86]

ADIAC functions as a voluntary, two-way partnership for information sharing between the private sector and the U.S. Government. According to TSA, ADIAC does not produce its own intelligence. Instead, it functions as a consumer of intelligence, receiving and digesting intelligence from approximately 17 different intelligence agencies, which it then distills and disseminates to its membership, as appropriate. ADIAC staff are to work with the intelligence community to distill relevant intelligence to the lowest level of classification possible. ADIAC then disseminates the classified or sensitive information to its members through secure communication portals, daily webinars (for unclassified and sensitive security information), and industry day events (for sharing classified intelligence).

With regard to ADIAC's dissemination of classified information to its membership, a senior TSA official stated that ADIAC staff routinely disseminate classified threat reports to U.S. air carriers.[87] For example, the official added that all global cargo air carriers have secure telephone connections and all major cargo air carriers have classified email capability that allow ADIAC personnel to send classified reports or contact them to relay any classified threat information that may directly affect their operations.[88] The senior TSA ADIAC official also stated that, in some cases, ADIAC members do not have the security infrastructure to support a classified briefing. In these cases, ADIAC members must either travel to TSA headquarters to access the secure briefing facilities or receive the

[86]ADIAC is a chartered membership organization. The charter dictates that membership is open only to U.S.-based entities. Member applicants must be nominated and approved by government and private sector coordinating councils. Approval is based upon intent and ability to contribute information, function in accordance with the ADIAC mission, and possession of a security clearance of Secret or higher. TSA serves as ADIAC's lead agency, providing ADIAC with physical space and equipment, while the DHS Office of Intelligence and Analysis serves as TSA's supporting agency with the intelligence community. ADIAC was sponsored by the Office of the Director of National Intelligence in 2016.

[87]According to the TSA ADIAC official, all ADIAC members have personnel with Secret clearance.

[88]The senior TSA ADIAC official added that three air carriers also have secure Homeland Security Data Network systems installed at their headquarters for reviewing classified threat reports up to the Secret level. The official also stated that ADIAC has no statutory, regulatory, or charter mission to provide threat intelligence warnings to civil aviation. Instead, the intelligence community agencies and the Office of the Director of National Intelligence have this responsibility.

information from TSA intelligence officers stationed at airports.[89] According to TSA, one air carrier has arranged for one of its personnel with a security clearance to visit TSA headquarters on a regularly scheduled basis to review the latest classified information. The senior TSA ADIAC official stated that he would like to see more air carriers (who lack this necessary infrastructure) develop a comparable work arrangement and encourages government agencies to expand their sponsorship of security clearances to critical industry partners. According to the senior ADIAC official, ADIAC also maintains secure Homeland Security Data Network workstations dedicated for ADIAC industry partner use and encourages all ADIAC industry members to conduct on-site intelligence sharing in the secure TSA ADIAC facility as their missions allow.

ADIAC staff also receive and anonymize reports from private sector companies to share with the membership under ATSA 2002 authorities for government and industry threat information sharing.[90] Examples could include observations from an air carrier's in-country staff around the world on developments in specific countries, such as civil unrest. According to TSA, reports cover a broad range of topics either directly or tangentially related to aviation. For example, we observed ADIAC officials sharing with members reports about locust swarms in Africa, which had the potential to obstruct an aircraft's visibility, and the potential for civil unrest throughout the Middle East in the wake of U.S. military action resulting in the death of Iranian Gen. Suleimani in January 2020.

As of January 2021, membership consisted of 39 government agencies and 67 U.S.-owned aviation industry organizations, from which nearly 558

[89]According to the senior TSA ADIAC official, ADIAC's facility at TSA headquarters was specifically designed to provide a centrally located secure facility for cleared air carrier personnel to review classified and unclassified threat intelligence.

[90]According to the senior TSA ADIAC official, ADIAC has no intelligence collections authorities or role and relays aviation threat-relevant information provided by industry to the appropriate agencies for awareness.

approved individuals participated in ADIAC in fiscal year 2020.[91] ADIAC also provides information to over 3,300 additional nonmember stakeholders via a sharing portal in the DHS Homeland Security Information Network, which provides sensitive, but unclassified information to those stakeholders.[92] In fiscal year 2020, ADIAC increased its membership by 50 percent and the products shared with industry by 15 percent.[93]

Conclusions

Over the past decade, terrorists have attempted to use air cargo shipments to smuggle concealed explosives into the United States, and TSA has determined that the risk to inbound air cargo security remains significant. Given this level of risk, TSA and CBP are aware of the importance of leveraging all relevant information to inform their air cargo risk assessment efforts and have coordinated the exchange of important and relevant information to maximize their assessments. However, TSA risk officials did not receive relevant ACAS trend data that might have enhanced their understanding of risks to air cargo risk security. Establishing a documented process for the exchange of applicable information between TSA and CBP that ensures all relevant parties are

[91]With respect to government agencies, we spoke to officials with the U.S. Postal Service regarding their information sharing experiences with CBP and TSA. The U.S. Postal Service officials stated that, while they have an excellent working relationship with both CBP and TSA, they have not made a request to TSA for membership in ADIAC. U.S. Postal Service officials explained that the agency has not seen a need to join ADIAC because its information sharing needs are being met through its ongoing collaboration with CBP officials on security issues. However, they may revisit membership if the need arises in the future. The U.S. Postal Service receives U.S.-bound mail after it enters the United States and, before delivering it within the United States, provides to CBP any mail that agency has requested for further inspection. After inspecting and clearing the selected mail, CBP releases it to the U.S. Postal Service for delivery within the United States.

[92]The Homeland Security Information Network is a web-based platform operated by the Department of Homeland Security to facilitate sensitive but unclassified information sharing and collaboration among federal, state, local, tribal, and private sector entities. DHS describes Homeland Security Information Network as its primary information-sharing mechanism. The Homeland Security Information Network is made up of a network of communities, called communities of interest. These communities are organized by state organizations, federal organizations, or mission areas such as emergency management and critical infrastructure.

[93]A senior TSA official stated that ADIAC gathers information annually from its membership on what they regard as their most important intelligence requirements (with respect to security information and air cargo security threats) to relay to the intelligence community and DHS.

aware of and receive key data, would provide greater assurance that TSA and CBP have fully optimized their air cargo risk assessments.

TSA's field assessment and ultimate qualification of a CT-based explosives detection system will provide a new type of technology to help airlines meet the requirement to screen 100 percent of air cargo traveling on passenger aircraft. However, TSA's CT field assessment did not follow guidance from key practices or the TSA T&E Guidebook, which TSA told us it uses to design all its field assessments. TSA did not collect essential data during the field assessment that would validate the CT system's ability to adequately detect explosive threats in the field. Without an independent test of the system's probability of detection, or a valid alternative testing method, during the field assessment, TSA cannot be assured that the CT system detects explosives threats in the field at a level consistent with prior laboratory testing and TSA requirements.

In addition, TSA did not consistently set performance thresholds or perform statistical analysis consistent with TSA T&E guidance for the data collected during the course of its field assessment. Without a statistical analysis that considers the measurement errors and performance thresholds and evaluates data against these thresholds to establish statistical confidence, TSA cannot establish whether the CT system has met TSA's requirements. TSA needs to accurately assess whether the system meets TSA's requirements to make a credible determination of whether the system should be designated as "qualified" on its air cargo screening technology list, which determines whether air carriers can use the system to screen cargo.

Recommendations for Executive Action

We are making the following four recommendations to DHS:

The Secretary of DHS should ensure that the Administrator of TSA and the Commissioner of CBP establish a documented process to ensure that relevant officials from both agencies are aware of and have access to applicable data to inform their inbound air cargo risk assessment efforts. (Recommendation 1)

The Administrator of TSA, prior to designating the explosives detection system for air cargo screening currently under evaluation as "qualified" on the air cargo screening technology list, should, to the extent practicable, verify through additional data collection or analysis that the system's

probability of detection in the field matches the performance measured in laboratory testing. (Recommendation 2)

The Administrator of TSA should ensure that necessary data are collected during field assessments to independently verify that the probability of detection of explosives detection systems for air cargo screening in the field matches the performance measured in laboratory testing, prior to designating systems as "qualified" on the air cargo screening technology list. TSA could provide this verification either through live explosives testing or, when operational considerations limit TSA's ability to use live threat materials, TSA should use an independently validated, fully documented alternative testing strategy. (Recommendation 3)

The Administrator of TSA should ensure statistical techniques are used to analyze data from TSA field assessments, including data from the current field assessment, of explosives detection systems for air cargo screening, prior to designating systems as "qualified" on the air cargo screening technology list. This statistical analysis should include the following elements:

- calculating error values for each quantitative measurement,
- identifying all necessary performance thresholds, and
- comparing the measured values and errors against each threshold to determine the statistical confidence of the results. (Recommendation 4)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and the U.S. Postal Service for review and comment. The U.S. Postal Service provided written comments, stating it did not have any further comment beyond technical comments previously provided, which we incorporated as appropriate. DHS also provided written comments, which are noted below and reproduced in full in appendix IV. DHS concurred with our four recommendations and described actions undertaken or planned to address them. DHS also provided technical comments, which we incorporated as appropriate.

With regard to our first recommendation that TSA and CBP establish a documented process to ensure relevant officials have access to applicable data to inform air cargo risk assessments, DHS concurred and stated that in January 2021, TSA and CBP officials discussed possible

data sources necessary to support improved risk analysis. They agreed to conduct a formal discussion to identify next steps, such as conducting a risk information exchange between TSA and CBP, identifying variables of interest and defining how best to exchange relevant information, and drafting a Memorandum of Understanding to guide the future exchange of relevant information. TSA and CBP estimated they would complete these tasks by February 28, 2022. These steps, if fully implemented, should address the intent of this recommendation.

With regard to our second and third recommendations that TSA verify that the probability of detection in the field matches the performance measured in laboratory testing, for both the CT system currently under evaluation and future systems, respectively, TSA concurred, and requested that we close the recommendations as implemented, based on actions taken. According to TSA, its actions over the course of the field assessment to verify probability of detection with image quality techniques—specifically the use of a manufacturer-developed operational test kit during its field assessment—are sufficient to ensure that probability of detection in the field matches system performance measured in the laboratory. We disagree with TSA's assessment.

As detailed in this report and reiterated in TSA's comments, TSA bases its evaluation of the system's probability of detection in the field on CT image quality tests performed by a manufacturer-developed operational test kit. Our findings clearly indicate that TSA's use of an operational test kit—without independent validation—is not an acceptable alternative to test the system's probability of detection in the field. While there is general industry acceptance of image quality testing for CT systems, to rely on a manufacturer-developed operational test kit to evaluate probability of detection in the field, TSA must independently validate that the operational test kit's results (1) correlate with the system's ability to detect threats (as measured in laboratory testing) and (2) accurately capture ways in which the system's performance could degrade.

TSA must also measure the performance of the kit using quantitative metrics. Officials at the Transportation Security Laboratory underscored the importance of independent validation when they told us that the performance of these kits can vary across manufacturers in their ability to detect deterioration in a CT system's performance. We found that TSA has not independently validated the operational test kit, instead relying on the manufacturer's design and analysis, and therefore, TSA should not solely rely on the operational test kit to verify CT system performance in the field. If TSA continues to rely on the operational test kit, independent

validation would play a critical role in helping TSA ensure the CT system's probability of detection performance in the field matches system performance measured in the laboratory.

We also found that TSA has not collected quantitative data from the operational test kit to assess the performance of the CT system. In its written comments on our draft report, TSA stated it has collected additional data from the operational test kit and plans to analyze those data using statistical methods. However, in the course of our review of TSA documents and multiple discussions with TSA officials regarding the CT field assessment, they provided no evidence that they had collected any quantitative data from the operational test kit or had any documented plans to analyze those data and compare them with data collected at the Transportation Security Laboratory.

Establishing an independent verification of the probability of detection during its field assessment is essential to ensuring the CT system has the ability to detect explosives threats in the field and, therefore, essential to fulfilling TSA's regulatory responsibilities. If TSA chooses to use image quality testing to accomplish this verification—through the operational test kit or any other means—it must provide evidence that it has independently validated the method it used and collected and analyzed quantitative data to evaluate the system's performance and establish that the system continues to meet probability of detection requirements in the field environment. These actions are necessary for TSA to address the intent of the recommendations.

With regard to our fourth recommendation that TSA use statistical techniques to analyze data from its field assessments, TSA concurred and requested that we close the recommendation as implemented based on planned actions. According to TSA officials, they intend to provide statistical analysis of some performance metrics after they collect sufficient data from the CT field assessment. While we are encouraged that TSA stated it has plans to conduct statistical analysis on data from its field assessment, we have been unable to substantiate that TSA's planned analysis will include all necessary statistical elements, as identified in our recommendation. Specifically, during the course of this review, TSA officials informed us they would include statistical analysis in their final field assessment report. However, despite multiple requests, TSA has yet to provide documentation—such as a data analysis plan—of its plans to evaluate metrics using a statistical analysis that would include all the elements identified in our recommendation.

TSA also stated that it did not set performance thresholds for some field assessment metrics because it did not need them to assess CT system performance in the field. We disagree. As previously discussed, TSA collected data on CT system clearance rates for different screening levels, and although TSA describes these metrics in its written comments as “indicative measures” that do not require performance thresholds, we have found that these metrics contain information about a key performance requirement, specifically, the false alarm rate.

We have noted how variations in false alarm rates, such as those that TSA observed in its field assessment, can indicate changes to the system’s core performance. Thus, establishing performance thresholds for these metrics would not be an “arbitrary constraint,” as TSA contends in its written comments, but would further ensure the CT system continues to meet key requirements when operating in a field environment. Furthermore, we also noted that TSA does evaluate these metrics qualitatively against the performance of CT systems used in its passenger checked baggage program, thus recognizing the necessity of comparing data measured in this field assessment against a performance standard.

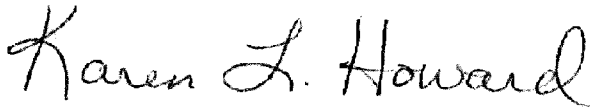
Therefore, we continue to believe it is necessary for TSA to evaluate data from the current and future CT field assessments with statistical techniques that establish a rigorous, scientific basis to determine whether a CT system meets TSA’s requirements. By providing a documented data analysis plan that identifies the statistical analysis performed to evaluate each metric, TSA would be better positioned to address the intent of the recommendation.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, the United States Postmaster General, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www/gao.gov.

If you or your staff have any questions concerning this report, please contact Triana McNeil at (202) 512-8777 or mcneilt@gao.gov or Karen L. Howard at (202) 512-6888 or howardk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on

the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Triana McNeil
Director, Homeland Security and Justice



Karen L. Howard, PhD
Director, Science, Technology Assessment, and Analytics

List of Committees

The Honorable Maria Cantwell
Chair
The Honorable Roger F. Wicker
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
The Honorable John Katko
Ranking Member
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report

1. Identifies the DHS programs that address U.S.-bound air cargo security and discusses how DHS measures their effectiveness;
2. Examines how DHS's ACAS program identifies high-risk U.S.-bound air cargo shipments;
3. Assesses the extent to which TSA and CBP have a documented process to ensure the full exchange of relevant information for assessing risk to inbound air cargo;
4. Assesses the extent to which TSA's air cargo computed tomography (CT) field assessment incorporated key practices for program design and evaluation; and
5. Identifies CBP and TSA's information-sharing procedures and practices for sharing threat information related to U.S.-bound air cargo with relevant stakeholders.

To identify which DHS programs address U.S.-bound air cargo security, we reviewed TSA and CBP documentation that detail requirements for passenger and all-cargo air carriers (both foreign and U.S.-flagged) that transport cargo into the United States.[1] We also reviewed TSA security directives and emergency amendments related to air cargo. We interviewed TSA and CBP officials regarding how these programs seek to ensure air cargo security. Specifically, we interviewed agency officials regarding (1) TSA's air cargo security requirements for the various classes of air carriers and cargo-related security directives and emergency amendments, (2) TSA's National Cargo Security Program (NCSP) Recognition Program, (3) TSA's air carrier inspection program, (4) TSA's airport assessment program, and (5) CBP's Air Cargo Advance Screening (ACAS) Program.[2]

For the ACAS program, we also obtained summary data for fiscal years 2017 through 2020 on the number of air carriers submitting required data,

[1]Air cargo includes freight and express packages that range in size from small to very large, and in type from perishables to machinery, and can include items such as electronic equipment, automobile parts, clothing, medical supplies, other dry goods, fresh cut flowers, fresh seafood, fresh produce, tropical fish, and human remains. Cargo can be shipped in various forms, including large containers known as unit loading devices that allow many packages to be consolidated into one container that can be loaded on an aircraft, wooden crates, assembled pallets, or individually wrapped/boxed pieces, known as "break-bulk" cargo.

[2]Throughout this report, we use the term "air carriers" to refer to both passenger and all-cargo air carriers that transport U.S. bound air cargo.

the number of those submissions reviewed by CBP's targeting personnel, and the number and types of ACAS referrals to air carriers for actions to be taken on shipments CBP identified as high risk. We chose these fiscal years because they covered the end of the ACAS pilot period and the first 2 years of full implementation. In assessing the reliability of these data fields, we conducted a site visit to CBP's National Targeting Center, reviewed documentation, and interviewed agency officials to collect information on data management practices and policies. We found these specific data fields from the ACAS module of CBP's Automated Targeting System database were sufficiently reliable to provide the cargo data submissions for each fiscal year and the number of those submissions identified for review and subsequent referrals.

To obtain insight on TSA's and CBP's air cargo security programs and requirements from the industry perspective, we selected two foreign international airports as a starting point for selecting air carriers to interview.[3] We selected these two airports based on (1) TSA's assessment of risk for these airports (either high or medium-high risk) and (2) the amount of cargo transported from these airports to the United States (i.e., these airports were among the top 25 worldwide in fiscal year 2017 for transporting air cargo into the United States). We reached out to nine air carriers that transported cargo from one or both of these airports to the United States based on fiscal year 2017 Bureau of Transportation Statistics data. We also interviewed three additional air carriers that, based on the fiscal year 2017 data, did not transport cargo from these two airports to the United States but were major air carriers worldwide, including transporting cargo to the United States. Of the 12 domestic and foreign-flagged air carriers we reached out to, we interviewed 11.[4]

We also spoke to TSA field personnel responsible for communicating with the foreign governments in these locations on air cargo security matters and other TSA officials serving as points of contact between the air carriers and TSA at these locations. We interviewed TSA field personnel at the agency's two Regional Operations Centers responsible for

[3]Because TSA deems the identity of these foreign airports to be sensitive information, we have omitted their names and geographic locations.

[4]One of the 12 carriers did not respond to our requests for an interview. We interviewed 10 air carriers by telephone and one through email. Because TSA deems the identities of these air carriers to be sensitive information, we have omitted their names.

conducting air carrier inspections and airport assessments.[5] We spoke to TSA field personnel to ascertain how they work with air carriers and foreign governments to ensure compliance with cargo security requirements, standards, and recommended practices. To obtain additional industry perspective on air cargo security-related issues and concerns, we interviewed the following associations: Airlines for America; Cargo Airline Association; Air Line Pilots Association, International; Coalition of Airline Pilots Associations; and the International Air Transport Association. We selected these associations based on input from TSA officials and based on the associations' specialized knowledge and experience with inbound air cargo security operations.

We also reviewed TSA's summary compliance results for the two foreign international airports to gain insight into the agency's compliance operations and air carriers' level of compliance with air cargo security requirements. We obtained summary results on TSA's air carrier inspections from TSA's Performance and Results Information System, and summary data on TSA's foreign airport assessments from the agency's Global Risk Analysis and Decision Support system. To assess the reliability of these data, we questioned knowledgeable TSA officials and reviewed relevant documentation regarding the databases and determined the data were sufficiently reliable for our purposes of gaining insight on air carriers' compliance with TSA air cargo security requirements.

To determine how TSA and CBP measure the effectiveness of their air cargo security programs and requirements, we reviewed summary data reports regarding the performance measures TSA developed in response to our 2019 report recommendations for the air carrier inspection, foreign airport assessment, and NCSP Recognition programs.[6] In conjunction with the review of summary data reports, we interviewed TSA officials regarding the tracking of the performance measures. We also reviewed the status of CBP's efforts to monitor ACAS program performance by reviewing summary reports of ACAS performance data for fiscal years 2017 through 2020. We reviewed relevant documentation and interviewed knowledgeable CBP officials regarding these data elements and

[5]TSA deems identifying information about the Regional Operating Centers responsible for conducting air carrier inspections and assessments at the two foreign airports we selected to be sensitive information; therefore, we do not identify the centers.

[6]GAO, *Aviation Security: TSA Uses a Variety of Methods to Secure U.S.-bound Air Cargo, but Could Do More to Assess their Effectiveness*, GAO-19-162 (Washington, D.C.: Nov. 28, 2018).

determined that these data were sufficiently reliable for our purposes of describing ACAS program performance. Lastly, we interviewed officials with TSA's Inspection Office regarding the status of covert testing at overseas locations to learn more about TSA's plans for assessing the effectiveness of the agency's air cargo security requirements for U.S.-bound cargo.

To examine how DHS's ACAS program identifies and assesses high-risk U.S.-bound air cargo shipments, we conducted an analysis of data on shipments, risk assessments, and action taken by CBP targeting personnel at the agency's National Targeting Center. Our data analysis was based on a random sample of 3,280,716 shipments, 2 percent of all US-bound air cargo shipments from calendar year 2019, provided by CBP. Because we followed a probability procedure based on random selections, the sample is only one of a large number of samples that might have been drawn. Since each sample could have provided different estimates, we express our confidence in the precision of this particular sample's results as a 95 percent confidence interval (e.g., plus or minus 2 percentage points). This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn. All estimates have 95 percent confidence intervals of +/- 0.007 percent or less, unless otherwise noted. We conducted a site visit to the National Targeting Center, reviewed documentation, and interviewed CBP headquarters and National Targeting Center officials to collect information on data management practices and policies. We found the data were sufficiently reliable for our purposes of characterizing the volume of cargo shipments and the risk management steps CBP targeting personnel performed.

To assess the extent to which TSA and CBP have a documented process for ensuring the full exchange of risk information between them, we reviewed the processes each agency uses to assess air cargo security risk. We reviewed relevant TSA and CBP documentation, such as classified and unclassified information, which included aviation threat scenarios and risk (threat, vulnerability, and consequence) ratings for foreign airports. We also interviewed TSA and CBP officials who are responsible for collecting and analyzing risk information and developing risk assessments; these included officials from TSA's International Risk Branch and from CBP's National Targeting Center. We assessed TSA and CBP risk assessment procedures against recommended practices in

DHS's *National Infrastructure Protection Plan* and *Risk Management Fundamentals*.[7]

To assess the extent to which TSA's CT field assessment incorporated key practices for program design and evaluation, we reviewed TSA's CT field assessment against key practices established from GAO guidance and TSA's *Test and Evaluation Guidebook* (T&E Guidebook).[8] In 2009, we recommended that TSA develop and document an evaluation plan for aviation security pilots.[9] TSA concurred and in 2012 TSA issued a memo outlining requirements for effective pilot evaluation based on five key practices laid out in our guide on designing program evaluations, which are:

1. Clarify understanding of the program's goals and strategy;
2. Develop relevant and useful evaluation questions;
3. Select an appropriate evaluation approach for each evaluation question;
4. Identify data sources and collection procedures to obtain relevant, credible information; and
5. Develop plans to analyze the data in ways that allow valid conclusions to be drawn from the evaluation questions.[10]

In September 2020, TSA officials told us that they follow the TSA T&E Guidebook as guidance for designing their qualification process and the field testing. Therefore, to evaluate the CT field assessment, we identified relevant sections of the T&E Guidebook for each key practice (see table 1). We reviewed documentation on the field assessment including the project plan, test plan, and monthly data analysis reports and conducted

[7]DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: Dec. 2013), and DHS, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: April 2011).

[8]GAO, *Designing Evaluations: 2012 Revision*, GAO-12-208G (Washington, D.C.: Jan. 2012).Transportation Security Administration, *Test and Evaluation Guidebook, Rev. 4* (Arlington, VA: Dec. 4, 2019).

[9]See GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009).

[10]Transportation Security Administration, Assistant Administrator, Office of Security Policy and Industry Engagement, *Requirements for Future Pilots, Projects and Programs*, Memorandum to Division Directors (Aug. 24, 2012); GAO, *Designing Evaluations: 2012 Revision*, GAO-12-208G (Washington, D.C.: Jan. 2012).

interviews with TSA officials. We used this evidence to compare TSA's CT field assessment against each key practice and the associated T&E guidance.

Table 1: Crosswalk of Government Accountability Office (GAO) Key Practices and Transportation Security Administration (TSA) Test and Evaluation Guidebook for the Computed Tomography Field Assessment

GAO Key Practice	Applicable TSA Test and Evaluation Guidebook Guidance
Clarify understanding of the programs goals and strategy	Section 3.3: Reviewing and Assessing Requirements
Develop relevant and useful evaluation questions	Section 3.5 Develop Evaluation Criteria
Select an appropriate evaluation approach or design for each evaluation question	Section 3.6 Test and Evaluation Master Plan Development Section 3.7 System Evaluation Plan
Identify data sources and collection procedures to obtain relevant, credible information	Section 6.2.1 Planning Documentation Section 6.2.2.1 Site Selection Working Group Develops Site Selection Criteria Section 6.4.1 Threat Inject Test Planning Section 6.5 Operational Test Data Authentication
Develop plans to analyze the data in ways that allow valid conclusions to be drawn from the evaluation questions	Section 3.10.5 System Evaluation Report "Memorandum on 'Test and Evaluation Statistical Methodology Policy for Probability of Detection and False Alarm Rate' Relevant Criteria" Section 6.2.1 Planning Documentation Section 6.4.1 Threat Inject Test Planning

Source: GAO analysis of TSA Test and Evaluation Guidance. | GAO-21-105192

We also interviewed officials with experience testing and developing standards for testing CT-based security screening systems. This included

- Officials at the Transportation Security Laboratory to obtain information about their process for certifying systems against TSA detection requirements and their work developing standards for image quality testing of CT-based explosives detection systems.[11]
- Officials at the National Institute of Standards and Technology who facilitated the development of the American National Standards Institute standard for image qualify testing of CT security-screening

[11]The Transportation Security Laboratory is a DHS Federal Laboratory that provides TSA with certification and qualification tests and laboratory assessments regarding screening technologies and their ability to detect explosives. It is part of DHS's Science and Technology Directorate, which is the Department's primary research and development arm.

systems[12] about their development of that standard and its possible application in field testing.[13]

- A former chair of the International Electrotechnical Commission's committee on standards for radiation protection instrumentation (SC 45B) who worked on the development of the International Electrotechnical Commission standard for image quality testing of CT security-screening systems about the development and proper implementation of that standard.[14]

To identify CBP and TSA's procedures and practices for sharing aviation-related threat information on U.S.-bound cargo, we interviewed CBP and TSA officials regarding procedures and practices each agency has in place for sharing such information with industry stakeholders. Specifically, for CBP, we interviewed officials, and reviewed related documentation, on the design and functionality of the Air Cargo Advanced Screening (ACAS) program with respect to how CBP's Automated Targeting System identifies high-risk cargo shipments and communicates with air carriers regarding those shipments.

For TSA, we interviewed officials with the agency's Aviation Domain Intelligence Integration and Analysis Cell (ADIAC) within the Intelligence and Analysis office regarding its methods for obtaining aviation-related threat information from government agencies (including the intelligence community) and sharing it with members of the aviation industry that carry U.S.-bound air cargo. We also interviewed officials and obtained and reviewed information from TSA on ADIAC's membership requirements and related processes in addition to its current membership levels. We also reviewed reports and attended webinar-based briefings for members to observe how ADIAC shares aviation-related intelligence with its membership. Lastly, we obtained and reviewed a member survey designed by ADIAC to obtain feedback from the membership on the cell's performance.

[12]Institute of Electrical and Electronics Engineers Standards Association, *American National Standard for Evaluating the Image Quality of X-ray Computed Tomography (CT) Security Screening Systems*. (New York, NY: May 23, 2011).

[13]*The Case for Technical-Performance Standards for Radiation Inspection Systems*, Larry Hudson, Journal of Testing and Evaluation 46 (2018) pp. 8-16. https://doi.org/10.1520/JTE20170329

[14]International Electrotechnical Commission, *Radiation protection instrumentation – Measuring the imaging performance of X-ray computed tomography (CT) security-screening systems.* (Geneva, Switzerland: Sept. 12, 2018).

We also interviewed officials with the U.S. Postal Service regarding their aviation security-related information sharing experiences with CBP and TSA.

We conducted this performance audit from January 2020 to May 2021 in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: TSA and CBP Air Cargo Security Programs

The Transportation Security Administration (TSA) and U.S. Customs and Border Protection (CBP) have multiple programs in place for the security of U.S.-bound air cargo. This appendix provides information on TSA's air cargo security requirements in addition to the various air cargo security programs both TSA and CBP have in place.

TSA's Cargo Security Requirements for Air Carriers

TSA has separate sets of security requirements based on whether the air carrier is domestic versus foreign-flagged or an all-cargo versus passenger carrier. These separate security requirements are shown in table 2 below.

Table 2: Transportation Security Administration (TSA) Security Requirements for Domestic and Foreign-Flagged Air Carriers

Security requirements for domestic air carriers	Security requirements apply to passenger carriers	Security requirements apply to all-cargo carriers
Aircraft Operator Standard Security Program	X	–
Full All-Cargo Aircraft Operator Standard Security Program	–	X
Security requirements for foreign air carriers		
Model Security Program	X	–
All-Cargo International Security Program	–	X

Source: GAO analysis of TSA air carrier security program requirements. | GAO-21-105192

Note: In addition to the security programs listed in this table, pursuant to the Aviation and Transportation Security Act, TSA established and oversees implementation of the Twelve-Five Standard Security Program. This program applies to aircraft weighing more than 12,500 pounds in scheduled or charter service that carry passengers, cargo, or both, and that do not fall under another security program.

For limited periods of time, TSA may also issue new or revised security requirements in the form of security directives or emergency amendments. These security directives and emergency amendments will eventually either expire (if there is a defined expiration date), be canceled (if, at any point, TSA deems it no longer necessary), or be incorporated as additional requirements in the air carriers' individual security programs, which they must follow. TSA's Aviation Division, within its Policy, Plans, and Engagement Office, is chiefly responsible for developing the security directives and emergency amendments with Cargo Division input. As of March 2021, nearly half of the TSA's aviation security directives and emergency amendments (22 of 48) were cargo-related (20 dealt exclusively with air cargo and 2 included air cargo as an element).

As part of its recent reorganization, TSA created the Air Cargo Division, under the Policy, Plans, and Engagement Office. The Air Cargo Division is responsible for developing, updating, and coordinating with industry on

air carrier security requirements encapsulated within the air carriers' individual security programs.[1] With regard to the Air Cargo Division's industry relationship, 10 of the domestic and foreign-flagged air carriers we interviewed were aware of TSA's Air Cargo Division, which the agency had reformed during its recent reorganization.[2] All 10 carriers expressed satisfaction with the assistance they received from the division—such as clarifications on regulatory language.

TSA's Air Carrier Inspection Program

TSA uses inspections to assess whether air carriers that transport cargo to the United States effectively implement TSA security requirements for their operations at foreign airports. TSA uses a multistep process to plan and conduct air carrier cargo inspections.

TSA plans inspections by first developing an annual Master Work Plan that TSA's regional operations centers use to schedule air carrier inspections each fiscal year. TSA separately plans for passenger carrier inspections and cargo carrier inspections.

In general, following a risk-informed approach, TSA conducts these compliance inspections either annually or semi-annually based on the risk level of the airport that is influenced, in part, by the airport's vulnerability to security breaches.[3] During the inspections, teams of TSA inspectors assess air carriers against security program requirements detailed in their security programs covering all six pillars of cargo supply chain security.[4] These six pillars are:

[1]Section 1943 of the TSA Modernization Act directed TSA to establish an air cargo security division to carry out and engage with stakeholders regarding the implementation of TSA air cargo security programs. Pub. L. No. 115-254, div. K, title I, subtitle D, § 1943, 132 Stat. 3186, 3584 (codified at 49 U.S.C. § 44947).TSA set up the new cargo division in a reorganization that was completed in December 2018. TSA previously had a cargo division that was eliminated as part of a prior reorganization in fiscal year 2014.

[2]We reached out to 12 carriers, of which eleven responded and agreed to be interviewed or responded to questions through email.

[3]TSA defines risk as a function of threat, vulnerability, and consequence and uses various data sources to assess airport risk, including: presence of threats and government control of corruption (threat); foreign airport and air carrier inspection results (vulnerability); and number of flights and average passenger load (consequence).

[4]The TSA inspection teams—based out of the TSA regional operations centers—generally include one team leader and one team member and typically take 1 or 2 days, but can involve more inspectors and take longer to complete depending on the extent of service by the air carrier. The inspectors may spend several days at a foreign airport inspecting carriers if there are multiple air carriers serving the United States from that location.

- **Facility security.** Procedures and mechanisms to prevent unauthorized entry to facilities where cargo is screened, prepared, and stored.
- **Chain of custody/transit procedures.** Methods or procedures to prevent and deter unauthorized access to cargo while stored or in transit between facilities prior to loading onboard aircraft.
- **Screening.** Screening of cargo through the application of technical or other means that are intended to identify weapons or explosives.
- **Personnel security.** Processes to vet individuals with unescorted access to air cargo at any point in the air cargo supply chain.
- **Training.** Training of personnel who screen, handle screened cargo, or perform other duties related to air cargo screening, preparation, or storage.
- **Compliance and oversight activities.** Clearly established requirements that regulated entities must satisfy to participate in a TSA-approved security program, and routine audits of such entities for compliance by TSA or appropriate authorities.

When conducting the inspections, TSA inspectors examine air carriers' implementation of applicable security requirements, including their TSA-approved security programs, any amendments or alternative procedures to these security programs, and applicable security directives or emergency amendments.[5] Compliance inspections can include reviews of documentation, such as security manuals or training and cargo screening logs; interviews of air carrier personnel; and direct observations of air cargo operations (including cargo acceptance and screening). TSA updates the inspections to reflect changes to TSA requirements and the current threat environment.

If an inspection results in a TSA inspector finding that an air carrier is not in compliance with any applicable security requirements, additional steps are to be taken to correct and record those specific violations, which can

[5]TSA inspectors may also evaluate air carriers' compliance with the cargo security program of a foreign country in which it operates if TSA has approved that country's program under its National Cargo Security Program (NCSP) Recognition Program. TSA's NCSP Recognition Program is discussed later in this section. TSA inspection teams are composed of "transportation security specialists," also referred to as "inspectors," who are primarily responsible for performing and reporting the results of both air carrier inspections and foreign airport assessments. Their responsibilities also include providing on-site assistance for making recommendations for security enhancements. TSA also deploys inspectors in response to specific security incidents and to monitor for identified threats.

include providing on-the-spot counseling for minor violations (e.g., an employee not displaying their identification) or opening an investigation if the violation is potentially more serious (such as inadequate screener training). Upon conclusion of the investigation and determination that a violation has occurred, TSA is to make a decision whether to issue a warning notice, letter of correction, or notice of proposed civil penalty.[6] If at the conclusion of the investigation TSA determines that a violation has not occurred, the agency will issue a "no action" letter to the air carrier.

Ten of the 11 air carriers we interviewed told us they had no significant issues complying with TSA's air cargo security requirements. Ten carriers also stated they had no problems responding to TSA inspection findings related to those requirements.[7] The air carriers also told us they had no problems working with TSA personnel regarding the requirements or results of the inspections. Specifically, these carriers stated they had good relationships with their assigned TSA International Industry Representatives—TSA's representatives to air carriers—and found them helpful in resolving or clarifying any issues that occur with respect to the cargo security requirements or findings from the inspections.[8]

[6]TSA takes administrative actions, which can include issuing a warning notice or letter of correction if the violation was unintentional or inadvertent, was not the result of a substantial disregard for security, and there are no prior cases involving similar violations resolved with administrative action. In addition, according to TSA, the air carrier may agree to develop an action plan to address the violation in lieu of a civil penalty. In these cases, the air carrier agrees to invest resources to address the issue leading to the violation instead of paying the penalty.

[7]One of the 11 air carriers indicated a number of difficulties complying with some of the security requirements including comments on the complexity of the TSA security manuals and confusion over differing requirements between passenger and all-cargo aircraft requirements. With regard to findings from TSA inspections, one of the 11 air carriers stated they had little contact with TSA—particularly with respect to the two international airports we selected for interviews with local officials. Because DHS deems the identity of the two foreign airports to be sensitive information, we have omitted their names and geographic locations.

[8]TSA international industry representatives are the primary point of contact between TSA and U.S. and foreign-flagged air carriers with last point-of-departure flights to the United States. These representatives provide guidance to air carriers on TSA regulations and help them meet their TSA-approved security program requirements. If TSA inspectors identify a security violation during an inspection, and it leads to an investigation, international industry representatives will coordinate with air carriers to ensure they take corrective action. In addition, international industry representatives serve as a liaison to air carriers during a security incident.

With regard to inspections performed by TSA at the two foreign airports we selected, the TSA International Industry Representatives for the cities in which these airports are located confirmed that none of the air carriers they were responsible for had any particular difficulty in complying with TSA's air cargo security requirements or responding to findings related to air carrier inspections. Summary inspections data provided by TSA for these airports showed four air carriers with last point-of-departure flights from one of the foreign airports during fiscal year 2019. Two of these air carriers had a single cargo-related violation in fiscal year 2019. The summary inspection data show that TSA resolved the issue with one air carrier through counseling and opened an investigation to review the finding for the other air carrier.

TSA's Foreign Airport Assessment Program

The International Civil Aviation Organization (ICAO), a specialized agency of the United Nations, is responsible for developing standards and recommended practices for international civil aviation.[9] These standards and recommended practices include ensuring that passengers and cargo are properly screened and that unauthorized individuals do not have access to restricted areas of the airport.[10] TSA inspection teams assess the foreign airports using 48 ICAO standards and recommended practices, including nine standards or practices that are specific to the acceptance, screening, and protection of cargo.[11]

TSA uses a risk-informed approach to schedule foreign airport assessments, generally every 1 to 3 years, with high-risk airports

[9]TSA inspection teams assess the foreign airports using ICAO standards and recommended practices, including standards or practices that are specific to the transport of cargo and mail. These standards include measures for the acceptance, screening, and protection of air cargo. More specifically, an ICAO standard is a specification for the safety or regularity of international air navigation, with which member states agree to comply; a recommended practice is any desirable specification for safety, regularity, or efficiency of international air navigation, with which member states are strongly encouraged to comply.

[10]See 49 U.S.C. § 44907(a)(2)(C). TSA utilizes select ICAO standards and recommended practices it sees as most critical to conduct its foreign airport assessments. TSA uses 48 standards and recommended practices detailed in Annex 17 to the Convention of International Civil Aviation, *Safeguarding International Civil Aviation Against Unlawful Acts of Interference,* Eleventh Edition, adopted November 25, 2019 and effective March 30, 2020, in addition to Annex 14, *Aerodrome Design and Operations,* Volume I.

[11]See 49 U.S.C. § 44907. TSA assesses foreign airports (1) served by a U.S. air carrier, (2) from which a foreign air carrier operates U.S.-bound flights, and (3) that pose a high risk of introducing danger to international air travel; as well as other foreign airports the Secretary of Homeland Security considers appropriate. See id. § 44907(a).

assessed more frequently than medium- to low-risk airports.[12] According to TSA, inspectors generally use the same process to plan and conduct airport assessments as air carrier inspections. Also, TSA generally performs both air carrier inspections and airport assessments during the same site visit. In these cases, the inspectors will use the results of the air carrier cargo inspections conducted earlier in the visit to inform the cargo portion of the airport assessment. At the end of each foreign airport assessment, TSA inspectors are to prepare a report detailing findings on the airport's overall security posture and security measures that may also contain recommendations for corrective actions.[13]

Although TSA is authorized under U.S. law to conduct foreign airport assessments at intervals it considers necessary, it may not perform an assessment of security measures at a foreign airport without permission from the host government. Also, TSA's airport assessments differ from its air carrier inspections in that, under the assessments, TSA does not have authority to impose or otherwise enforce security requirements at foreign airports. Instead, TSA must work with host government civil aviation officials to both schedule the airport visits and improve conditions when deficiencies are identified in the assessments.

We spoke to the TSA Representatives (who communicate with foreign governments regarding transportation security matters) for the two foreign airports we selected about their interactions with the local governments regarding TSA's airport assessments and the airports' adherence to ICAO standards and recommended practices for air cargo.[14] The TSA Representatives for both airports stated that government officials

[12]Tier 1 airports—airports that are determined to be low risk—are generally assessed once every 3 years. Tier 2 airports—airports determined to be medium risk—are generally assessed every 2 years. Tier 3 airports—those determined to be high risk—are generally assessed annually.

[13]According to TSA, their inspectors' post-airport assessment reporting also includes all of the measures that the foreign airport conducted satisfactorily in accordance with the ICAO standards and recommended practices that were assessed during the visit.

[14]TSA representatives communicate with foreign government officials to address transportation security matters and to facilitate foreign airport assessments. TSA representatives also serve as on-site coordinators for TSA responses to terrorist incidents and threats to U.S. assets at foreign transportation modes. For the foreign airport assessment program, TSA representatives are often involved in arranging pre-assessment activities, assessment visits, and follow-up visits. Additionally, TSA representatives are responsible for helping host government officials address security deficiencies that are identified during assessments. The ICAO standards and recommended practices for air cargo include measures for the acceptance, screening, and protection of air cargo.

representing the countries in which the two airports are located were very proactive in employing technology and processes and procedures related to air cargo security (to comply with selected ICAO standards and recommended practices identified by TSA). According to the TSA Representatives, both governments are willing to invest resources to ensure their airports are up to date with respect to addressing security needs based on TSA requirements. Neither TSA Representative reported any recent cargo-related findings for the airport assessments for these two airports. As a result, the TSA Representatives stated that they have not needed to interact with local government officials on these types of matters. TSA airport assessment summary data confirmed that its inspectors did not identify any cargo-specific findings at either airport as a result of the most recent assessments.

TSA's National Cargo Security Program Recognition Program

National Cargo Security Program (NCSP) recognition is a voluntary agreement between TSA and a foreign government to recognize the foreign country's air cargo security program. The agreement enables air carriers to follow the country's program in lieu of their individual TSA-approved security programs.[15] TSA's NCSP recognition process involves three phases: (1) a technical review and analysis of a foreign country's air cargo security program's requirements with TSA requirements to determine if the country's program aligns with TSA practices; (2) validation visits to the foreign country to determine if the air cargo security program aligns with TSA practices; and (3) a decision on whether to recognize the foreign government's air cargo security program as commensurate with TSA's air cargo security requirements. The recognition decision is based on whether the foreign government's NCSP is commensurate with TSA requirements across TSA's six pillars of cargo supply chain security. The potential outcomes are as follows: (1) recognition with no caveats, (2) recognition with caveats, and (3) recognition not granted.[16] In cases where recognition is not granted, TSA will make recommendations to that government on how to improve its air cargo security program to better align with TSA and global air cargo security requirements.

[15]According to TSA, air carriers must request an amendment to their individual, TSA-approved security programs that allow them to follow the foreign country's air cargo security program.

[16]TSA's six pillars of cargo supply chain security include facility security, chain of custody/transit procedures, screening, personnel security, training, and compliance and oversight activities.

According to TSA, the NCSP Recognition Program benefits U.S. inbound air cargo security because it (1) increases its visibility into recognized governments' air cargo security requirements and air cargo supply chains, (2) facilitates the identification of air cargo industry vulnerabilities, and (3) is a key component of TSA's efforts to achieve 100 percent screening of U.S.-bound air cargo and enhance global supply chain security.

TSA Monitoring of the NCSP Recognition Program

According to NCSP documentation, once TSA determines a foreign government's security program is commensurate with TSA requirements and NCSP recognition is granted to that country, it monitors NCSP implementation through air carrier cargo inspections, foreign airport assessments, ongoing engagements with foreign government officials, and revalidation of NCSP recognition. As a result of these monitoring activities, TSA may decide to revalidate the country's approved security program on either a continuous or time-limited basis (historically every 3 years). According to TSA, these monitoring activities may also result in the termination of the approval of a country's security program under the NCSP.[17]

According to NCSP documentation, after its initial creation in 2010, TSA periodically reviewed the approved security programs of the countries approved under the program every 3 years. In December 2016, TSA altered the NCSP recognition framework to include a "grant-and-monitor" process for sustaining NCSP recognitions (referred to as Continuous Recognition), which offers an alternative to the structured time-limited grant of recognition to allow recognitions to be granted without a specified time limit but subject to continuous monitoring over the life of the recognition.

Further, according to NCSP documentation, TSA's grant-and-monitor approach is contingent upon the host country's maintenance of security measures and arrangements in place between it and TSA. These arrangements include: the commitment to regular engagements between TSA and the host government appropriate authority to share program changes and security updates; regular and routine compliance inspections and assessments of airports throughout the host country, to include other regulated supply chain entities (that may be located off-airport); and ongoing programmatic reviews to ensure a commensurate

[17]In countries without NCSP recognition, air carriers transporting air cargo into the United States from last point-of-departure airports must continue to apply their TSA-approved security program requirements pertaining to cargo.

level of security is maintained between the U.S. and each country's respective NCSPs. Under continuous recognition, countries must still continue to meet the Terms of Recognition outlined in the TSA-issued letter of recognition, and must continue to allow the conduct of TSA's foreign airport assessment and air carrier security inspection visits.

Status of TSA's NCSP Recognition Efforts

As of January 2021, TSA had recognized the air cargo security programs of the European Union (27 member countries) and 14 other countries.[18] In addition, TSA is currently working with three countries that have yet to be fully evaluated and recognized for participation—Argentina, Turkey, and Taiwan.

Relationship of NCSP Recognition Program to TSA's Canine Security Program

Countries approved under the NCSP Recognition Program are also eligible to implement TSA's Canine Security Program.[19] TSA assesses the canine programs of foreign countries to determine if they are commensurate with TSA's requirements for screening air cargo, passengers, and checked baggage.

TSA considers the Canine Security Program to be intertwined with the NCSP Recognition Program and uses the same three phases to assess commensurability of foreign canine security programs that it uses for the NCSP Recognition Program. However, the Canine Security Program has separate security "pillars" from the NCSP and requires some specialized expertise with regard to assessing each country's critical security pillars, which include looking at such aspects as training, handling and regulation of explosives training aides, and the country's oversight and compliance process.

As of February 2021, TSA had recognized the canine security programs of the European Union, the United Kingdom, and New Zealand. According to TSA officials, they are continuing to develop the program. As

[18]Of these countries, only Canada, Israel, and Norway have no "caveats" to their approved security programs under the NCSP. When TSA recognizes a country's program with caveats, TSA requires air carriers transporting cargo from that country to continue to implement specific TSA requirements on U.S.-bound flights because certain aspects of the country's security program are not in line with those requirements. According to TSA officials, caveats are often based on specific threats or vulnerabilities. Further, most caveats are due to the fact that a country is unable to legally require that a specific procedure be completed because of national legislation or international norms.

[19]According to TSA, a country cannot have an approved canine program without first having an approved air cargo security program under the NCSP Recognition Program.

of May 2020, Canada and South Africa were in the process of applying to TSA for approval of their respective canine security programs.

CBP's Air Cargo Advance Screening (ACAS) Program

CBP uses its Automated Targeting System (ATS) to identify potentially high-risk cargo for review and possible referral to the air carrier for further action. A referral may consist of (1) a request from CBP to the carrier for more information on the shipment, (2) a request that the carrier perform the required screening on the shipment as outlined in the carrier's TSA-approved security program, or (3) a do not load order.[20] CBP has yet to issue a "do not load" order for any shipment—this order would forbid air carriers from loading cargo, which may contain an explosive device, onto the aircraft.[21]

We reached out to 12 select domestic and foreign-flagged air carriers regarding their experiences with ACAS, and interviewed officials from 11 of them. Of the officials from the 11 carriers we spoke to, all generally indicated positive experiences with ACAS referrals.[22] However, 5 of the 11 air carriers noted occasional delays in CBP notifying them of the resolution of a referral and release of the hold on a shipment.

CBP officials explained that there are several possible reasons why an air carrier may not realize a hold has been lifted. The first is that an air carrier may not be familiar with the coding CBP uses to denote a released shipment. The CBP officials added that they provide this coding to all air carriers by way of the ACAS Implementation Guide.[23] The second reason air carriers may not realize a hold has been lifted is that some have recently experienced technical problems with their internet service providers (and is therefore not attributable to ACAS). Lastly, CBP officials stated that, in some cases where there are two referrals on the same shipment (e.g., both a request for additional information and a directive to the carrier to conduct screening), the air carrier may satisfy one referral

[20]CBP officials clarified that, for referrals where TSA directs the air carrier to perform required screening, it is not necessary for the carriers to perform additional screening if the carrier has already performed the TSA-required screening on the shipment in question. In these cases, the air carrier provides CBP personnel with a statement confirming that enhanced screening was completed on the cargo.

[21]Because DHS deemed the number of ACAS referrals made from fiscal years 2017 through 2020 to be sensitive, we have omitted these data.

[22]One of the 12 carriers did not respond to our inquiries.

[23]U.S. Customs and Border Protection, *Implementation Guide—Air Cargo Advance Screening (ACAS)* (Washington, D.C.: July 2019).

but not realize there is a second referral on the same shipment. In these cases, the air carrier expects CBP to lift the hold and that notification never comes due to the remaining, unresolved referral.

According to the CBP officials, CBP's Office of Information Technology held technical conference calls every week since the beginning of the ACAS pilot until June 2020 (approximately 2 years after issuance of the interim final rule). The Office of Information Technology is now holding these conference calls once a month to address issues such as this. These calls are open to all air carriers and other ACAS participants that wish to participate. They expect this forum to continue to provide a means for the air carriers to resolve such issues as they occur.

Appendix III: Analyzing Explosives Detection Systems with Receiver Operating Characteristic (ROC)

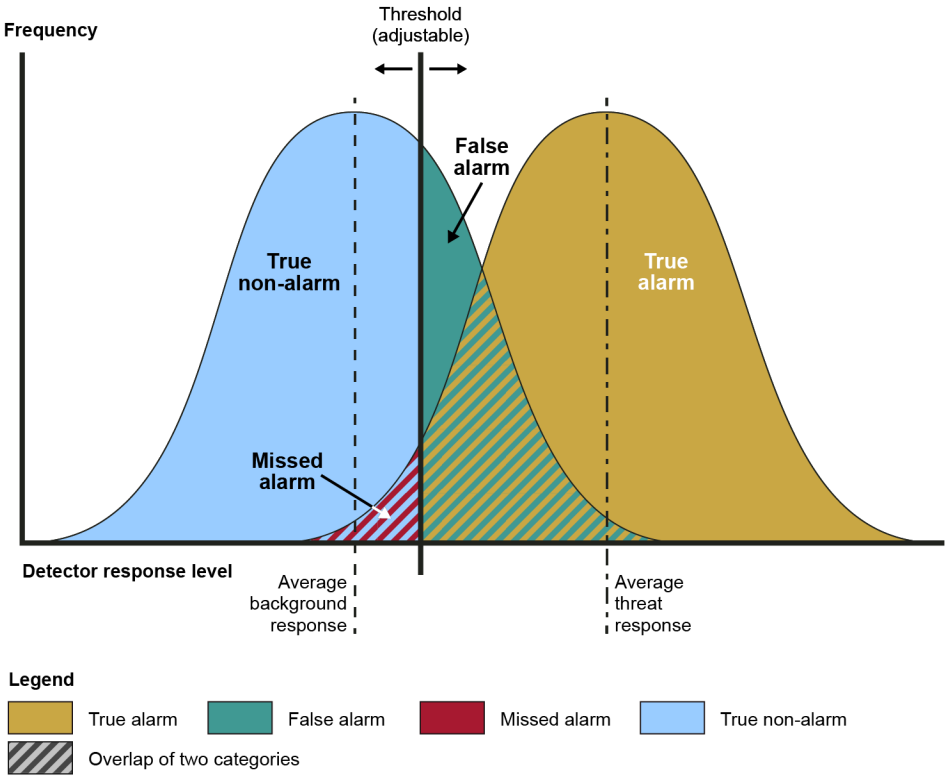
The ROC is an analysis tool to study the relationship in a system's performance between the false alarm rate and the probability of detection. Designers and users of these systems can use this information to optimize a system's performance and understand the impact of external factors, such as a change in background.

Principle of ROC

ROC has found many applications for systems that make a binary decision (yes/no, threat/no-threat, positive/negative) including security screening systems and medical tests. These systems will measure an external stimulus and produce a response signal. They try to use that response signal to determine what external stimulus caused the response: a real threat or background noise from the environment.[1] Figure 5 shows how a simplified system might produce a response signal to background sources versus real threats. Both background and real threats can produce a range of responses due to statistical variations and small variations in the system. To distinguish threats from background, the operator of the system will then set a threshold at a certain response level. All responses above that threshold will be considered as threats and all responses below that threshold disregarded.

[1]This appendix will consistently use the terms "threat"/"no-threat" when discussing ROC, but the same principles and analysis apply to other systems, which might return a positive/negative response or other binary response.

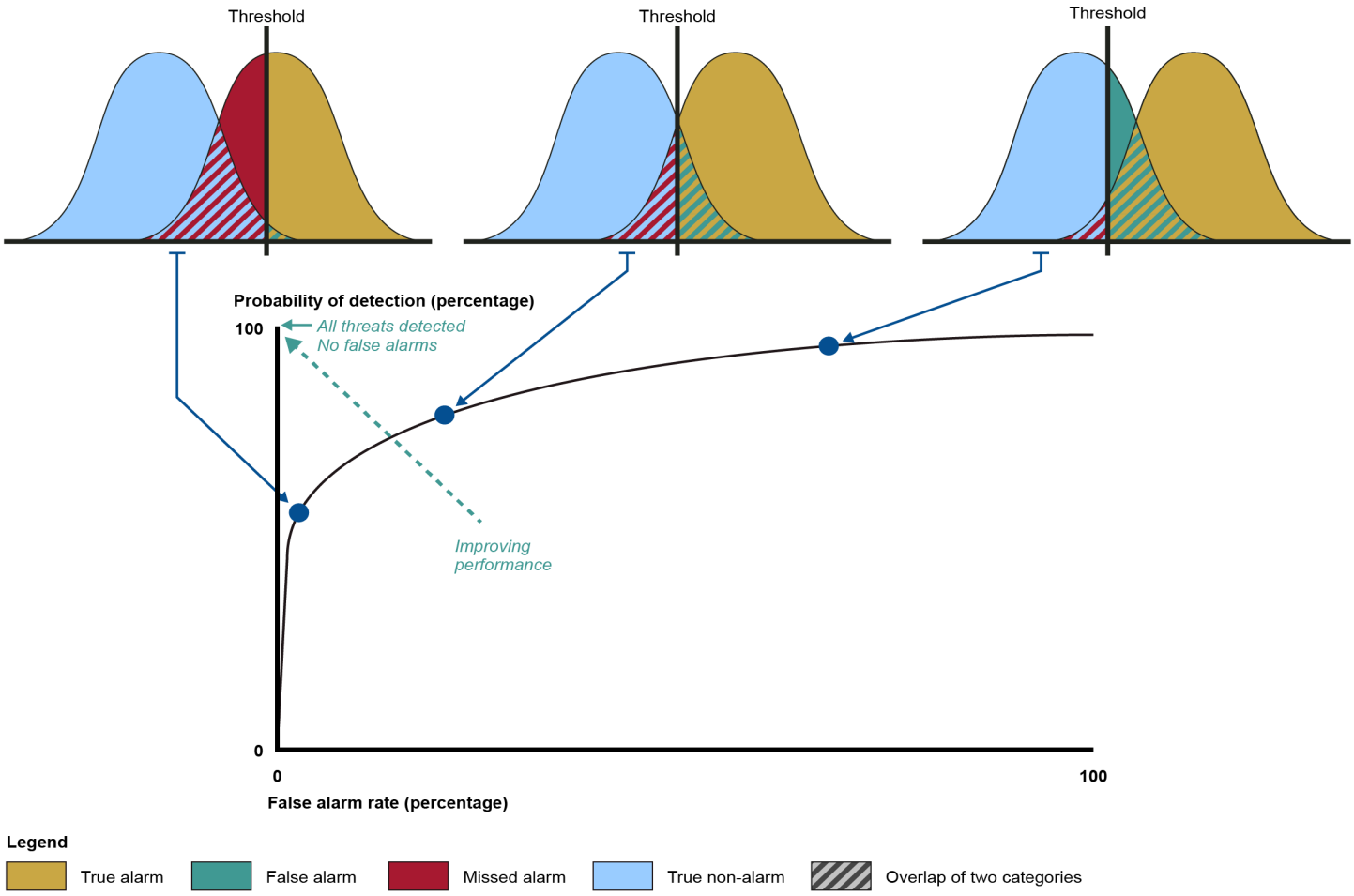
Figure 5: A Simplified Model of a System's Response to Background and Threat



Source: GAO analysis of technical literature. | GAO-21-105192

Due to the range of system responses for background and threats, a natural tradeoff will exist between the system's ability to detect threats (probability of detection) and the number of background events that will be incorrectly interpreted as threats (false alarm rate). For example, lowering the threshold will allow the system to detect more real threats but will also increase the number of false alarms. To understand the tradeoff for a given system, the operator can vary the threshold level and measure the false alarm rate and probability of detection at each threshold level. These results can be plotted as the probability of detection versus the false alarm rate to visually show the relationship between the two for a given system. This plot is the ROC curve (see fig. 6).

Figure 6: A Receiver Operating Characteristic (ROC) Curve Displaying the System's Probability of Detection and False Alarm Rates for Different Thresholds



Source: GAO analysis of technical literature. | GAO-21-105192

The shape of the curve depends upon the system's ability to discriminate between background and threat (the separation between the two peaks in fig. 5). The closer the curve approaches the upper left corner of the plot, the better overall discriminating power the system has. The ROC curve also allows the operator to decide on ideal settings between false alarm rate and probability of detection and understand how changes in one parameter will trade off with the other.

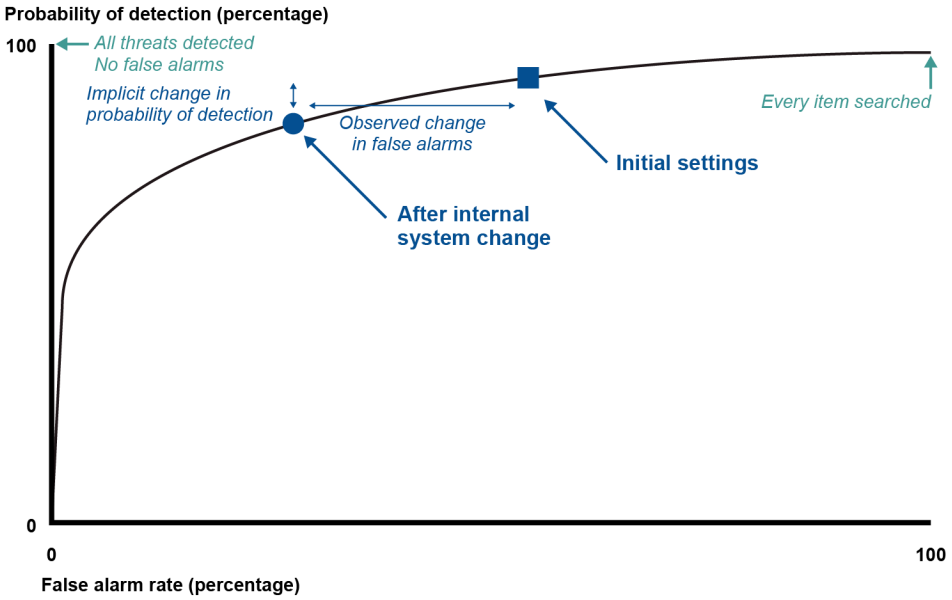
Application to the Transportation Security Administration's (TSA) Testing of Explosives Detection System Technology

Understanding the ROC of a system can provide important information about the operational effectiveness of a system. The tradeoff between false alarm rate and probability of detection will relate to important operational tradeoffs for TSA and the end user. While a higher probability of detection will ensure the system detects more explosive threats, it will also come with a greater number of false alarms, which will require more time and operators to check and clear those alarms.

TSA sets a false alarm and probability of detection threshold that the system must meet in the laboratory, but as previously discussed, has observed different false alarm rates in the field and faces challenges to measure the probability of detection in the field. A ROC analysis could serve as a tool to understand the holistic system performance and any variations observed in the field. Here are two examples of how a ROC could illustrate changes in the system's performance.

Example 1. First, if a change occurred in the system (e.g., change to an internal setting) that altered the system's threshold, it would be reflected by a change in the system's location on the ROC curve (see fig. 7). In the field, where the majority of parcels do not have a threat, the operator might observe this effect as a change in the false alarm rate, but would not know what impact this change had on the probability of detection. However, by previously measuring the ROC curve for this system in the laboratory, the user could infer the approximate change in the probability of detection from the change in false alarm rate.

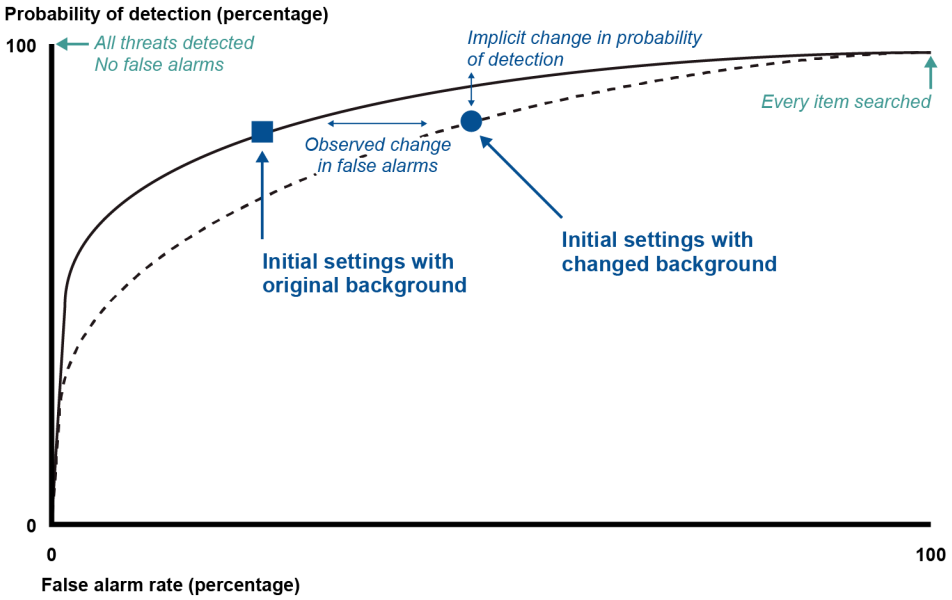
Figure 7: A Receiver Operating Characteristic (ROC) Curve Showing the Impact of a Change in the System's Internal Settings



Source: GAO analysis of technical literature. | GAO-21-105192

Example 2. If, on the other hand, the system threshold remains the same but the parcels screened by the machine produce a different response (e.g. a change in the background curve), the discrimination power of the system could worsen. This would be reflected in a change in the entire shape of the ROC curve because the discrimination between the background and the threat has changed. This might result because the background as tested in a laboratory is not representative of the background in the field environment. Again, this would appear to the operator as a change in the false alarm rate. However, the ROC curve would allow the user to understand the change in the tradeoff between the probability of detection and the false alarm rate (see fig. 8). The user could use this information from the ROC curve to re-optimize the system's performance in the presence of the new background. In this example, the ROC curve could be calculated by collecting a representative set of data for the new background response and performing modeling and numerical analysis of the system.

Figure 8: A Receiver Operating Characteristic (ROC) Curve Showing the Impact of a Change in Background



Source: GAO analysis of technical literature. | GAO-21-105192

Appendix IV: Comments from the Department of Homeland Security (DHS)

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 20, 2021

Triana McNeil
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-21-105192, "AIR CARGO SECURITY: TSA Field Testing Should Ensure Screening Systems Meet Detection Standards"

Dear Ms. McNeil:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased that GAO recognizes the importance of the Transportation Security Administration's (TSA) and U.S. Customs and Border Protection (CBP) programs for ensuring the security of air cargo transported to the United States, and both Components have taken steps to measure their effectiveness. It is important to note, however, that TSA's air cargo program has different responsibilities than designated acquisition programs. Specifically, TSA's air cargo program is regulatory in nature, as opposed to its acquisition efforts which assess air cargo marketplace technologies through the Air Cargo Screening Qualification Test (ACSQT). Since its establishment in 2008, pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), TSA's ACSQT program has been very successful in enhancing air cargo security and, as a result of the program, the air carrier industry is investing significant amounts of resources in ACSQT qualified technologies. DHS remains committed to fully meeting its air cargo security mission responsibilities.

The draft report contained four recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO'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. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2021.07.20 12:38:56 -04'00'

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-21-105192

GAO recommended that the Secretary of DHS ensure that the Administrator of TSA and the Commissioner of CBP:

Recommendation 1: Establish a documented process to ensure that relevant officials from both agencies are aware of and have access to applicable data to inform their inbound air cargo risk assessment efforts.

Response: Concur. On October 22, 2020, TSA's Risk Branch met with TSA staff embedded at the CBP National Targeting Center (NTC) to identify possible data sources to enhance risk analysis. During January 2021, CBP and TSA staff discussed possible data sources necessary to support improved risk analysis and agreed that a formal discussion including CBP Headquarters personnel would be the next step in evaluating how to implement the recommendation. Moving forward, TSA anticipates:

- Conducting a CBP-TSA risk information exchange;
- Conducting a classified discussion on NTC and data variables;
- Identifying variables of interest to both CBP and TSA and defining how best to exchange information; and
- Drafting a Memorandum of Understanding for information exchange, as appropriate

Estimated Completion Date: February 28, 2022.

GAO recommended that the Administrator of TSA:

Recommendation 2: Prior to designating the explosives detection system for air cargo screening currently under evaluation as "qualified" on the air cargo screening technology list, should, to the extent practical, verify through additional data collection or analysis that the system's probability of detection in the field matches the performance measured in laboratory testing.

Response: Concur. TSA already verifies that an explosives detection system's probability of detection in the field matches the performance measured in laboratory testing using Computed Tomography (CT) image quality comparative analysis. Specifically, Certification Testing at the Transportation Security Lab (TSL) is the approved location for testing with live explosives, which is done on a "per Explosives Detection System (EDS) configuration basis." Testing with live explosives in the field carries too much risk; therefore, TSA verifies EDS performance through various

3

independent and non-independent test methods that are performed on each system. These include:

- The American National Standards Institute (ANSI) N42.45 Standard for Evaluating the Image Quality of X-ray Computed Tomography Security-Screening Systems test articles run during Factory Acceptance Testing (FAT); and
- Original Equipment Manufacturer (OEM) specific Operational Test Kits (OTKs) run routinely in the field.

This methodology is consistent and applicable for EDS for both the Air Cargo and the Electronic Baggage Screening Program (EBSP).

The ANSI N42.45 National Standard, dated May 23, 2011, is a methodology to evaluate the image quality of a CT-based EDS, and therefore verify that the probability of an EDS' detection in the field matches the tests performed during certification testing in the laboratory. The N42.45 test articles track metrics for object length accuracy, path length CT value and Z-effective, noise equivalent quanta, CT value consistency, CT value uniformity, and X-ray energy spectrum consistency, streak artifacts, slice sensitivity profile, and image registration. Although not all metrics are applicable to all designs of CT, FATs utilizes the Image Quality – Factory Acceptance Test articles which comply with the ANSI Standard.

OTKs are vendor designed test articles, engineered for demands for daily use, which must be run at least once every 24 hours or after maintenance activities. An automated OTK analysis software algorithm is embedded within each EDS to provide the user a positive indication of image quality compliance and, therefore, device readiness to perform screening functions. The specific metrics each vendor selects to extract from the OTK are consistent with a subset of the measurements performed under the N42.45 standard. Each vendor selects those measurements which are most sensitive to change for their unique system and are therefore likely to indicate a negative change in image quality performance. Understandably, vendors do not want to incur the cost of including unnecessary components in the design of their OTK, and the selection of test articles which represent the most sensitive measurements is a reasonable compromise.

N42.45 provides the mechanism and methodology to compare an EDS in the field to the "gold standard" EDS that underwent certification testing at the TSL. Comparison can be performed on a complete or subset of metrics derived from test articles, such as an OTK. A nonparametric test of equality, such as a Kolmogorov-Smirnov test can compare these one-dimensional probability distributions with statistical confidence to establish a fielded EDS provided the same image quality as the certified example. Such analysis is conducted for the current field assessment, for which equality is established.

We request that the GAO consider this recommendation closed, as implemented.

4

Recommendation 3: Ensure that necessary data are collected during field assessments to independently verify that the probability of detection of explosive detection systems for air cargo screening in the field matches the performance measured in laboratory testing, prior to designating systems as "qualified" on the air cargo screening technology list. TSA could provide this verification either through live explosives testing or, when operational considerations limit TSA's ability to use live threat materials, TSA should use an independently validated, fully documented alternative testing strategy.

Response: Concur. As testing with live explosives in the field carries too much risk, TSA's Air Cargo Qualification Program will continue to rely on the ANSI N42.25 National Standard, as appropriate, to verify the probability of detection of EDS for air cargo screening in the field. The program will also accept vendor designed OTK which can demonstrate compliance with necessary measurements from the N42.45 standard as an acceptable alternate testing methodology.

We request that the GAO consider this recommendation closed, as implemented.

Recommendation 4: Ensure statistical techniques are used to analyze data from TSA field assessments, including data from the current field assessment, of explosives detection systems for air cargo screening, prior to designating systems as "qualified" on the air cargo screening technology list. This statistical analysis should include the following elements:

- calculating error values for each quantitative measurement,
- identifying all necessary performance thresholds, and
- comparing the measured values and errors against each threshold to determine the statistical confidence of the results.

Response: Concur. TSA's Air Cargo Qualification Program already conducts quantitative measurements related to EDS suitability, which possess identified performance thresholds and statistical confidence requirements and must be met before device qualification. Further, it is important to note that measurements related to operational effectiveness do not require performance thresholds. These are indicative measures for inputs into the air cargo operator's labor and cost model to support their acquisition decision.

The Air Cargo Qualification Program and EBSP conduct field assessments differently. This is necessary because the EBSP field assessment, known as operational test and evaluation, is a component of an acquisition decision, whereas the Air Cargo field assessment focuses on EDS compliance with the Functional Requirements Document (FRD). As air cargo field assessments are conducted in partnership with the OEM and an air cargo operator, the TSA Air Cargo Qualification Program does not purchase the

equipment under test and the EDS may be provided by the OEM or purchased by the air cargo operator. In addition, the EDS is installed in the air cargo operator's facility.

Air Cargo field assessments focus on the suitability and the effectiveness of the EDS in an operational setting. Specifically, data collected on operational utilization and preventive and corrective maintenance actions allows the TSA Air Cargo Qualification Program to calculate the reliability, maintainability and availability (RMA) metrics. Consequently, the EDS undergoing field assessment is considered a representative sample of the population for all EDS of this type (i.e., model under configuration management). Robust statistical analyses can be conducted after sufficient operational utilization, which is established by the qualification program to be at least twelve months and is the decision point for compliance with RMA requirements as defined in the FRD. RMA-related quantitative measurements will also be analyzed with statistical confidence as defined in the FRD.

Analysis conducted in support of operational effectiveness metrics is performed by the TSA Air Cargo Qualification Program to ensure EDS in Air Cargo are performing a function commensurate with EBSP and to provide an indicative measure to air cargo operators in support of their acquisition decisions. Operational effectiveness measures are automatically recorded by the technology at each level in the screening process, and a hard performance threshold exists requiring all parcels to have all alarms resolved before completing the screening process. The percentage of commerce that cannot be cleared at each screening level may be a function of one or more criteria, such as "Level 1 (EDS) Alarm Rate," "EDS Image Quality," "Level 2 Operator Staffing," "Level 2 Operator Competency," and "Level 2 Auto Divert Timing," some of which are independent of the device under qualification, but are nevertheless important inputs to the operational modeling conducted by the air cargo operator when making a procurement decision.

TSA believes that assignment of an arbitrary constraint, or performance threshold, on any given individual measure of operational effectiveness is inappropriate, as it would be optimal to only one operational model. It is important to permit air cargo operators to optimize their screening operations within the constraints of the regulated screening program, and that operational effectiveness measures be calculated and presented in each final report along with statistical variance measures where appropriate to support air cargo operators with their procurement decisions and site planning.

We request that the GAO consider this recommendation closed, as implemented.

6

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Triana McNeil at (202) 512-8777 or mcneilt@gao.gov.

Karen L. Howard at (202) 512-6888 or howardk@gao.gov.

Staff Acknowledgments

In addition to the individuals named above, Taka Ariga (Chief Data Scientist), Kevin Heinz (Assistant Director), Barbara Guffy (Analyst-in-Charge), William Bauder, Dominick Dale, Michele Fejfar, R. Scott Fletcher, Eric Hauswirth, Michael Harmond, Andrew Kurtzman, Thomas Lombardi, Dennis Mayo, Benjamin Moser, Sasan J. “Jon” Najmi, and Sarah Williamson made key contributions to this report. Katie Hamer and Ardith Spence also contributed to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.