Privacy Impact Assessment

for the

TSA Air Cargo Programs

DHS Reference No. DHS/TSA/PIA-019(c)

January 5, 2022

Homeland Security

Abstract

The Transportation Security Administration (TSA) conducts security threat assessments on individuals working within the transportation sector. TSA's regulation of the air cargo industry includes requirements for security threat assessments on individuals who have or are applying for unescorted access to air cargo, that are principals and owners of companies applying for TSA certification, or have air cargo screening-related duties. The TSA air cargo requirements are implemented through several programs that cover various aspects of air cargo preparation, screening, and transportation. This Privacy Impact Assessment (PIA) is being conducted in accordance with Section 222 of the Homeland Security Act of 2002, codified at 6 U.S.C. 142. It updates, consolidates, and supersedes prior Air Cargo PIAs conducted on April 14, 2006, and November 12, 2008.

Overview

Air Cargo Security

TSA has broad authority to ensure the adequacy of security measures for the transportation of cargo,[1] as well as authorities relating more specifically to air cargo.[2] Among its efforts for air cargo security, TSA promulgated regulations that require 100 percent screening of air cargo transported on passenger aircraft[3] and developed the Certified Cargo Screening Standard Security Program to provide an approved method for the screening of air cargo.[4] For all of its air cargo programs, TSA requires individuals to undergo a recurrent security threat assessment (STA) in order to screen cargo; access facilities that store, screen, or secure cargo; have unescorted access to cargo; perform duties as an air cargo security coordinator; or hold a supervisory role over individuals who perform these functions. TSA also requires security threat assessments for individuals who have ownership or financial interests in an Indirect Air Carrier (IAC)[5] and Certified Cargo Screening Facility (CCSF).

A security threat assessment is an inquiry to confirm an individual's identity and determine whether the individual poses or may pose a security or terrorist threat to transportation or the Nation. The components of the security threat assessment will vary depending on the program but may include a check against intelligence and transnational organized crime databases for indications that the individual may pose a threat to national security or of terrorism; a check against

[1] *See* 49 U.S.C. § 114(f)(10).
[2] 49 U.S.C § 44901(a), (f), and (g).
[3] Air Cargo Security Requirements; Final Rule, 71 FR 20478 (May 26, 2006).
[4] Air Cargo Screening; Interim Final Rule, 74 FR 47672 (Sept. 16, 2009) and Air Cargo Screening; Final Rule, 76 FR 51848 (Aug. 18, 2011).
[5] An Indirect Air Carrier is any person or entity within the United States, not in possession of a Federal Aviation Administration air carrier operating certificate, which undertakes to engage indirectly in air transportation of property and uses for all or any part of such transportation the services of an air carrier (49 CFR § 1540.5).

law enforcement databases (such as those maintained by the Treasury Department Office of Foreign Assets Control or the U.S. Marshals Service) for disqualifying offenses; and an immigration database check. The appendix to this Privacy Impact Assessment provides a table describing the TSA cargo programs and the security threat assessment elements that are required for each. Air cargo program immigration checks are performed against the U.S. Citizenship and Immigration Service (USCIS) Systematic Alien Verification for Entitlements (SAVE) database,[6] and may also include VISA revocations or other databases.

Finally, some individuals subject to air cargo security requirements may also fall within other TSA programs that require a security threat assessment with requirements more fully described within Privacy Impact Assessments applicable to those programs. The other TSA programs may require different components for the security threat assessment, such as a fingerprint-based criminal history record check that requires the applicant to submit fingerprints to TSA for checks against Federal Bureau of Investigation (FBI) criminal history records. For example, air cargo handlers working within an airport may be required to obtain an airport issued badge to access secured areas and will be required to submit information for that access badge.[7]

Known Shipper Management System

TSA also requires aircraft operators, foreign air carriers, and indirect air carriers to conduct known shipper programs as required by their TSA-approved security programs.[8] Through the Known Shipper Management System (KSMS), TSA identifies and approves the known shipper status for qualified shippers to be able to transport their cargo on passenger aircraft. Aircraft operators, foreign air carriers, and indirect air carriers must comply with a range of specific security requirements to qualify their clients as "known shippers." Shippers interested in transporting goods by air may contact their transportation service provider and request to become a known shipper. TSA collects identifying information to build the known shipper database for regulated parties, such as indirect air carriers, aircraft operators and foreign air carriers. While most known shippers are corporate entities, TSA recognizes that some individuals may also qualify as known shippers. In such cases, TSA requires the indirect air carrier, aircraft operator, or foreign air carrier to conduct a site visit of the known shipper as well as a Known Shipper Management System check with Dun & Bradstreet[9] to validate the entity.

---

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS PROGRAM, DHS/USCIS/PIA-006, *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE AIRPORT ACCESS FOR AVIATION WORKERS, DHS/TSA/PIA-020, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[8] See 49 CFR parts 1544, 1546, and 1548.

[9] Dun & Bradstreet is a corporation that offers information and reports on businesses. Most notably, Dun & Bradstreet is recognizable for its Data Universal Numbering System (DUNS numbers); these generate business information reports for more than 100 million companies worldwide.

Section 1.0 Authorities and Other Requirements

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

Under the Aviation and Transportation Security Act (ATSA) and authority delegated from the Secretary of Homeland Security, TSA is responsible for security in all modes of transportation.[10] TSA is required to provide for screening cargo that will be carried aboard passenger aircraft, and establish a system to screen, inspect, or otherwise ensure the security of all cargo that is to be transported in cargo aircraft.[11] In 2018, Congress required TSA "to develop and issue standards for the use of … third party explosives detection canine assets for the primary screening of air cargo; and develop a process to identify qualified non-federal entities that will certify canine assets."[12]

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

Security threat assessments are covered by DHS/TSA-002 Transportation Security Threat Assessment System.[13]

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

Yes. The TSA Screening Gateway[14] was most recently granted an Authority to Operate (ATO) on 9/17/2019. The TSA Transportation Vetting System[15] (renamed Vetting and Credentialing System (VCS)) is in Ongoing Authorization. In addition, the Known Shipper Management System and the Indirect Air Carrier Management System (IACMS) are in Ongoing Authorization.

---

[10] 49 U.S.C. § 114(d).
[11] 49 USC §§ 44901(a) and (f).
[12] *See* § 1941 of the *TSA Modernization Act*¸ Div. K of the *FAA Reauthorization Act of 2018* (Pub. L. 115-254 (Oct. 5, 2018; 132 Stat. 3186).
[13] *See* DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (Aug. 11, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE VETTING AND CREDENTIALING SCREENING GATEWAY SYSTEM, DHS/TSA/PIA-001, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TECHNOLOGY INFRASTRUCTURE MODERNIZATION PROGRAM, DHS/TSA/PIA-042, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

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

Yes. National Archives and Records Administration approved retention and disposal policy N1-560-06 applies to these records.

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

OMB Control Number: 1652-0040, Air Cargo Security Requirements.

Forms(s): Aviation Security Known Shipper Verification Form (TSA Form 419H), and Aircraft Operator or Air Carrier Reporting, and Security Threat Assessment Application (TSA Form 419F).

OMB Control Number: 1652-0053, Certified Cargo Screening Program.

Forms(s): The forms used for this collection of information include Letter of Intent (TSA Form 419A); Certified Cargo Screening Facility Profile Application (TSA Form 419B); Certified Cargo Screening Facility Principal Attestation (TSA Form 419D); Certified Cargo Screening Facility Security Profile (TSA Form 419E); and the Security Threat Assessment Application (TSA Form 419F).

Section 2.0 Characterization of the Information

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

TSA collects information from regulated operators for individuals seeking or performing a variety of cargo handling functions under several programs more specifically identified in the appendix. The following information is collected on individuals on whom a security threat assessment is conducted for cargo security programs:

1. Legal name, including first, middle, and last; any applicable suffix; and any other names used;
2. Current mailing address, including residential address if different than current mailing address, and all other residential addresses for the previous five years and email address, if applicable;
3. Gender;
4. Date and place of birth;

5. Social security number (SSN);[16]
6. Citizenship status, and date of naturalization if the individual is a naturalized citizen of the United States;
7. A-number or Form I-94 Arrival/Departure Number, if the individual is not a U.S. citizen;
8. Daytime phone number;
9. Name, address, and telephone number of the individual's employer; and
10. Whether the Indirect Air Carrier Principals[17] reside within the United States.

In addition to the information listed above, TSA will collect and maintain information that an individual chooses to submit in connection with an appeal of a TSA determination, such as letters from a prosecutor, documents from a board of pardons, police documents, or other relevant documents. TSA will also maintain results of checks it performs against intelligence, law enforcement, and immigration databases in the course of performing the security threat assessment.

In some cases, an individual may have successfully completed a security threat assessment conducted by another government agency, and this security threat assessment may be acceptable for the air cargo program. If the individual asserts completion of a comparable threat assessment in lieu of a new security threat assessment, the individual should submit the name of the program for which the comparable threat assessment was conducted and the date on which it was completed.

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

Individual applicants will electronically submit their information directly to TSA for the security threat assessment. Information collected in the course of conducting the security threat assessment necessarily comes from other government agencies (e.g., Federal Bureau of Investigation criminal history records).

[16] Although provision of one's social security number is voluntary, failure to provide a Social Security number may result in delays or prevent completion of the security threat assessment.

[17] Defined as proprietor, general partner, officer, director, or owner of the entity. Owner means a person who directly or indirectly own, controls, or has power to vote 25 percent or more of any class of voting securities or other voting interests of an Indirect Air Carrier or applicant to be an Indirect Air Carrier; or a person who directly or indirectly controls in any manner the election of a majority of the directors (or individuals exercising similar functions) of an Indirect Air Carrier, or applicant to be an Indirect Air Carrier.

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

Dun & Bradstreet checks are conducted on "known shippers" to validate the business entity. Publicly available data may also be used during the security threat assessment or subsequent investigations. For example, public social media posts by an individual seeking or holding air cargo access may be relevant to the security threat assessment.

2.4 Discuss how accuracy of the data is ensured.

TSA relies on the accuracy of the information provided to it by the individual applicant and by the agencies whose databases are checked during the security threat assessment process. Individuals affected by a TSA decision regarding the security threat assessment may seek access to their records under the Privacy Act, and have additional opportunities for redress as specified in Section 7 below.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that an applicant may be incorrectly identified as a match to information contained in intelligence databases during the security threat assessment process.

Mitigation: This risk is mitigated. TSA reduces this risk by requiring data elements that should be sufficient to distinguish most applicants from individuals who are identified as a match to information contained in intelligence databases. TSA further reduces the risk by working directly with the individual to resolve any potential error in identification.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

TSA uses the information provided to conduct security threat assessments on personnel seeking or holding regulated access to cargo to determine whether they pose a security risk. TSA will run recurrent checks against intelligence, law enforcement, and immigration status databases to identify individuals who pose or are suspected of being a risk to transportation or national security. Individual information may be shared with third parties during the course of a security threat assessment or adjudication of a waiver or appeal, to the extent necessary to obtain information pertinent to the assessment or adjudication of the applicant or in accordance with the routine uses identified in the DHS/TSA-002 system of records notice. In addition, TSA may enroll biometrics and associated biographic data within the DHS Office of Biometric Information

Management Homeland Advanced Recognition Technology System (HART)[18] (formerly known as the Automated Biometric Identification System (IDENT)).

TSA also uses known shipper information to operate the Known Shipper Management System to assist Indirect Air Carriers and air carriers with identifying known shippers that have been previously qualified by other Indirect Air Carriers or air carriers.

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

No, while TSA conducts subject-based searches in the course of conducting the security threat assessment, it does not use technology to discover or locate predictive patterns or anomalies.

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

TSA shares the information within DHS in the course of conducting security threat assessments, including with the U.S. Citizenship and Immigration Service Systematic Alien Verification for Entitlements system to conduct immigration status checks and the Office of Biometric Information Management's Homeland Advanced Recognition Technology System.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII may be accessed or used inappropriately.

Mitigation: This risk is mitigated. PII collected by TSA will be used only in accordance with the described uses by integrating administrative, technical, and physical security controls that place limitations on the collection of PII, and protect PII against unauthorized disclosure, use, modification, or destruction. For example, TSA uses role-based access in its systems to ensure that individuals are only able to access data for which they have a need to know.

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART), DHS/OBIM/PIA-004, *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

Section 4.0 Notice

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

TSA provides a Privacy Act Statement under 5 USC 552a(e)(3) to individuals seeking a security threat assessment. Further, TSA has published regulations (as footnoted above) covering the air cargo populations. In addition, this PIA provides general notice to the public.

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

Individuals seeking covered access to air cargo voluntarily provide their personal information, but once provided, they cannot limit its uses by the program. Individuals may opt out (decline to provide information), but individuals who opt out will not receive an approved security threat assessment.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not know how their information is used.

Mitigation: The risk is mitigated. Through the information provided by TSA at the time of application through a Privacy Act Statement, as well as this PIA and the DHS/TSA-002 system of records notice, TSA provides sufficient notice to individuals.

Privacy Risk: Individuals may not be aware that their information will be vetted via the Homeland Advanced Recognition Technology System.

Mitigation: This risk is partially mitigated. Notice of sharing biographic and biometric information with the Homeland Advanced Recognition Technology System for recurring checks against intelligence, law enforcement, and immigration status databases is provided in this PIA. The Privacy Act Statement provided to individuals at the time they submit their information also gives express notice that TSA will conduct recurrent checks as part of the security threat assessment. Although individuals may not know that their biometrics are specifically shared with the Homeland Advanced Recognition Technology System, they should have a general understanding that their fingerprints are being used for vetting checks given that the individual provides their fingerprints directly to TSA for security threat assessment.

Section 5.0 Data Retention by the Project

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

TSA will retain records regarding individuals undergoing a security threat assessment in accordance with National Archives and Records Administration approved retention and disposal policy N1-560-06 as follows:

- TSA will delete or destroy information one year after it is notified that the individual's credential or access privilege, which was granted based upon the security threat assessment, is no longer valid.
- In addition, for those individuals who may originally have appeared to be a match to a government watchlist, but are later determined not to pose a threat to transportation or national security, retained information will be destroyed seven years after completion of the security threat assessment, or one year after any credential or access privilege granted based on the security threat assessment is no longer valid, whichever is longer.
- Information on individuals that are actual matches to a government watchlist or otherwise pose a threat to transportation or national security, will be deleted or destroyed ninety-nine years after completion of the security threat assessment, or seven years after TSA learns that the individual is deceased, whichever is shorter.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information is retained for longer than necessary.

Mitigation: This risk is mitigated. TSA will retain these records in accordance with the records retention schedule approved by the National Archives and Records Administration. TSA implements both physical and, where feasible, technical controls to implement proper retention periods.

Section 6.0 Information Sharing

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

Results of the security threat assessment will be shared with the air cargo operator regarding their employees and contractors. The information will be shared with the Federal Bureau of Investigation for individuals for whom TSA conducts criminal history records checks, and with the Threat Screening Center (TSC) to resolve possible watchlist matches. TSA may also share the information it receives with federal, state, or local law enforcement, immigration, or intelligence

agencies or other organizations, in accordance with the routine uses identified in DHS/TSA-002 Transportation Security Threat Assessment System of Records. Known shipper information will be shared within the Known Shipper Management System with users of the system (i.e., Indirect Air Carriers, air operators and foreign air carriers).

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

DHS/TSA-002 Transportation Security Threat Assessment System of Records, Routine Use I permits disclosure "to the appropriate federal, state, local, tribal, territorial, or foreign agency regarding individuals who pose, or are suspected of posing, a risk to transportation or national security." This is compatible with the collection of information for purposes of conducting security threat assessments since the Threat Screening Center is the multi-agency center that maintains the Terrorist Screening Database (TSDB) and the Federal Bureau of Investigation performs the Criminal History Record Checks.

Routine Use K permits disclosure "to a federal, state, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a DHS/TSA decision concerning an initial or recurrent security threat assessment…." This is compatible with the original collection to conduct the security threat assessment.

Routine Use N permits disclosure "to airport operators, aircraft operators, maritime and surface transportation operators, indirect air carriers, and other facility operators about individuals who are their employees, job applicants or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities when relevant to such employment, application, contract, training, or the issuance of such credentials or clearances." This is compatible with the original collection for purposes of conducting a security threat assessment.

6.3 Does the project place limitations on re-dissemination?

TSA does not place limitations on re-dissemination of information except to the extent information is Sensitive Security Information (SSI) pursuant to regulations involving non-disclosure of security information.[19] Sensitive Security Information may only be shared with covered persons with a need to know as defined by 49 C.F.R. part 1520.11.

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

Disclosures may either be recorded manually within investigative files or automatically in

[19] 49 U.S.C. § 114(r), November 19, 2001.

an output report the system produces.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be inappropriately shared.

Mitigation: This risk is mitigated. TSA may share this information in accordance with the Privacy Act. TSA mitigates attendant privacy risk by sharing externally only in accordance with published routine uses under the applicable SORN: DHS/TSA-002. Further, TSA has entered into a Memorandum of Understanding (MOU) with the Federal Bureau of Investigation and Threat Screening Center governing conditions of sharing information related to security threat assessment programs.

Section 7.0 Redress

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

An individual may request access to his or her data under the Privacy Act by contacting TSA Headquarters Freedom of Information Act (FOIA) Office under procedures available at www.tsa.gov/FOIA, or by writing to FOIA Officer, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6002.

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

Individuals may seek to correct information through a Privacy Act request as described in Section 7.1 of this PIA. In addition, individuals may appeal their security threat assessment following procedures set out in 49 CFR Part 1515.5 or 49 CFR Part 1515.9, as applicable. Individuals may also seek judicial review.

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

TSA will provide information on the procedures for correcting information with its determination; also, this PIA provides notice on how to correct information held by TSA. In addition, TSA provides information on how to submit a Privacy Act Request at www.tsa.gov/FOIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to correct, access, or amend inaccurate information maintained by TSA.

Mitigation: This risk is mitigated. Individuals are provided with the opportunity to access,

correct, or amend inaccurate information about them through the redress procedures described above. In addition, individuals may seek access to TSA records by submitting a request under the Privacy Act or under FOIA, though some aspects of their record may be exempt from access as stipulated in the DHS/TSA-002 Final Rule.[20]

Section 8.0 Auditing and Accountability

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

System administrators, security administrators, IT specialists, vetting operators, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based assess controls are employed to limit access to information by different users and administrators based on their need to know the information for the performance of their official duties. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. Program management was involved in the conduct and approval of this Privacy Impact Assessment.

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

All TSA employees are required to complete the annual DHS privacy training. In addition, security training is required, which raises the level of awareness and understanding for protecting personally identifiable information.

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

Only TSA employees and contractors with proper security credentials and passwords, and a need to know in order to fulfill their duties associated with conducting security threat assessments will have access to this information. All access is provided via system administrators or other designated personnel.

[20] *See* Final Rule for Privacy Act Exemptions, 69 FR 35536 (June 25, 2004), *available at* https://www.dhs.gov/system-records-notices-sorns.

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

TSA does not anticipate that information collected for this project will implicate any additional information sharing, uses, or access, but to the extent it does, they are controlled in accordance with Sections 8.1 and 8.3, and will be reviewed for compliance with this Privacy Impact Assessment.

Contact Official

John Beckius
Executive Director
Air Cargo Division
DHS/TSA
John.Beckius@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
DHS/TSA
TSAPrivacy@tsa.dhs.gov

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix

Security Threat Assessment components for individuals under Air Cargo programs

Program	Function	Intelligence	Law Enforcement	Immigration Status
12-5 Standard Security Program in an All-Cargo Operation	14 CFR Part 135 aircraft operator certified by the Federal Aviation Administration operating aircraft with a maximum certificated takeoff weight of more than 5670 kg (12,500 pounds) in an all-cargo operation	X	X (including fingerprint-based Criminal History Record Check)	
All-Cargo Twelve-Five International Security Program	14 CFR Part 129 aircraft operator certified by the FAA operating aircraft with a maximum certificated takeoff weight of more than 5670 kg (12,500 pounds) in an all-cargo operation. For cargo personnel located in the United States.	X	X	X
Full All-Cargo Aircraft Operator Standard Security Program	14 CFR Part 119 aircraft operator certificated by FAA operating aircraft with a maximum certificated takeoff weight of more than 45,500 kg (100,309.3 pounds) carrying cargo and authorized persons and no passengers	X	X (including fingerprint-based Criminal History Record Check)	X

All-Cargo International Security Program	14 CFR Part 129 foreign air carrier conducting all-cargo operations in aircraft with a maximum certificated takeoff weight of more than 45,500 kg (100,309.3 pounds) within the U.S., from the U.S. to a non-U.S. location, from a non-U.S. location serving as the last point of departure to the United States, and if stated in the All-Cargo International Security Program, overflying the United States. For cargo personnel located in the United States.	X	X	X
Indirect Air Cargo Standard Security Program	Indirect Air Carriers are persons or entities within the United States, not in possession of a Federal Aviation Administration air carrier operating certificate, which undertake to engage indirectly in air transportation of property and uses for all or any part of such transportation the services of an air carrier.	X	X	X
Secured Packing Facility	An Indirect Air Carrier operating as a Secure Packing Facility to secure cargo departing	X	X	X

	from the United States to non-U.S. locations on all-cargo aircraft			
Certified Cargo Screening Facility Programs	Cargo screening facilities located throughout the United States to screen cargo prior to providing it to airlines for transport on passenger flights.	X	X	X
Third-Party Canine-Cargo program	Third-party explosives detection canine team providers registered as a Certified Cargo Screening Facility-Canine; and third-party certifiers who determine whether canine teams meet TSA's certification requirements	X	X (except certain Certified Cargo Screening Facility - K9 employees must get a fingerprint-based Criminal History Record Check[21])	X

[21] Fingerprint-based Criminal History Record Check are required for Principal/Alternate Security Coordinators, employees/authorized representatives/immediate supervisors with unescorted access to screened cargo, and employees/authorized representatives/immediate supervisors authorized by the Certified Cargo Screening Facility-K9 to perform cargo screening as a canine team handler or supervisor.