Code of Federal Regulations

49

Part 1200 to End

Revised as of October 1, 2009

Transportation

Containing a codification of documents of general applicability and future effect

As of October 1, 2009

With Ancillaries

Published by
Office of the Federal Register
National Archives and Records
Administration

A Special Edition of the Federal Register

U.S. GOVERNMENT OFFICIAL EDITION NOTICE

Legal Status and Use of Seals and Logos

The seal of the National Archives and Records Administration (NARA) authenticates the Code of Federal Regulations (CFR) as the official codification of Federal regulations established under the Federal Register Act. Under the provisions of 44 U.S.C. 1507, the contents of the CFR, a special edition of the Federal Register, shall be judicially noticed. The CFR is prima facie evidence of the original documents published in the Federal Register (44 U.S.C. 1510).

It is prohibited to use NARA's official seal and the stylized Code of Federal Regulations logo on any republication of this material without the express, written permission of the Archivist of the United States or the Archivist's designee. Any person using NARA's official seals and logos in a manner inconsistent with the provisions of 36 CFR part 1200 is subject to the penalties specified in 18 U.S.C. 506, 701, and 1017.

Use of ISBN Prefix

This is the Official U.S. Government edition of this publication and is herein identified to certify its authenticity. Use of the 0–16 ISBN prefix is for U.S. Government Printing Office Official Editions only. The Superintendent of Documents of the U.S. Government Printing Office requests that any reprinted edition clearly be labeled as a copy of the authentic work with a new ISBN.

U.S. GOVERNMENT PRINTING OFFICE

U.S. Superintendent of Documents • Washington, DC 20402–0001

http://bookstore.gpo.gov

Phone: toll-free (866) 512-1800; DC area (202) 512-1800

Title 49—Transportation

(This book contains part 1200 to end)

SUBTITLE B—OTHER REGULATIONS RELATING TO TRANSPORTATION (CONTINUED)

Subtitle B—Other Regulations Relating to Transportation (Continued)

CHAPTER XII—TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

EDITORIAL NOTE: Nomenclature changes to chapter XII appear at 68 FR 49720, Aug. 19, 2003.

SUBCHAPTER A—ADMINISTRATIVE AND PROCEDURAL RULES

SUBCHAPTER B—SECURITY RULES FOR ALL MODES OF TRANSPORTATION

SUBCHAPTER C—CIVIL AVIATION SECURITY

SUBCHAPTER D—MARITIME AND LAND TRANSPORTATION SECURITY

SUBCHAPTER A—ADMINISTRATIVE AND PROCEDURAL RULES

PART 1500—APPLICABILITY, TERMS, AND ABBREVIATIONS

Sec.
1500.1 Applicability.
1500.3 Terms and abbreviations used in this chapter.
1500.5 Rules of construction.

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

SOURCE: 67 FR 8351, Feb. 22, 2002, unless otherwise noted.

§ 1500.1 Applicability.

This chapter, this subchapter, and this part apply to all matters regulated by the Transportation Security Administration.

§ 1500.3 Terms and abbreviations used in this chapter.

As used in this chapter:

Administrator means the Under Secretary of Transportation for Security identified in 49 U.S.C. 114(b) who serves as the Administrator of the Transportation Security Administration.

Person means an individual, corporation, company, association, firm, partnership, society, joint-stock company, or governmental authority. It includes a trustee, receiver, assignee, successor, or similar representative of any of them.

Transportation Security Regulations (TSR) means the regulations issued by the Transportation Security Administration, in title 49 of the Code of Federal Regulations, chapter XII, which includes parts 1500 through 1699.

TSA means the Transportation Security Administration.

United States, in a geographical sense, means the States of the United States, the District of Columbia, and territories and possessions of the United States, including the territorial sea and the overlying airspace.

[67 FR 8351, Feb. 22, 2002, as amended at 68 FR 49720, Aug. 19, 2003]

§ 1500.5 Rules of construction.

(a) In this chapter, unless the context requires otherwise:

(1) Words importing the singular include the plural.

(2) Words importing the plural include the singular.

(3) Words importing the masculine gender include the feminine.

(b) In this chapter, the word:

(1) ''Must'' is used in an imperative sense;

(2) ''May'' is used in a permissive sense to state authority or permission to do the act prescribed, and the words ''no person may * * *'' or ''a person may not * * *'' mean that no person is required, authorized, or permitted to do the act prescribed; and

(3) ''Includes'' means ''includes but is not limited to''.

PART 1502—ORGANIZATION, FUNCTIONS, AND PROCEDURES

AUTHORITY: 5 U.S.C. 3345, 49 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44920, 44935–44936, 44942, 46101–46105, 45107, 46110.

SOURCE: 67 FR 48049, July 23, 2002, unless otherwise noted.

§ 1502.1 Responsibilities of the Administrator.

(a) The Administrator is responsible for the planning, direction, and control of the Transportation Security Administration (TSA) and for security in all modes of transportation. The Administrator's responsibility includes carrying out chapter 449 of title 49, United States Code, relating to civil aviation security, and related research and development activities, and security responsibilities over other modes of transportation that are exercised by the Department of Transportation.

(b) The Deputy Administrator is the ''first assistant'' to the Administrator for purposes of the Federal Vacancies Reform Act of 1998, and shall, in the event the Administrator dies, resigns, or is otherwise unable to perform the functions and duties of the office, serve as the Acting Administrator, subject to the limitations in the Federal Vacancies Reform Act of 1998. In the event of the absence or disability of both the

Administrator and the Deputy Administrator, officials designated by TSA's internal order on succession shall serve as Acting Deputy Administrator and shall perform the duties of the Administrator, except for any non-delegable statutory and/or regulatory duties.

PART 1503—INVESTIGATIVE AND ENFORCEMENT PROCEDURES

Subpart A [Reserved]

Subpart B—Scope of Investigative and Enforcement Procedures

Sec.

Subpart C—Investigative Procedures

Subpart D—Non-Civil Penalty Enforcement

Subpart E—Assessment of Civil Penalties by TSA

Subpart F [Reserved]

Subpart G—Rules of Practice in TSA Civil Penalty Actions

Subpart H—Judicial Assessment of Civil Penalties

Subpart I—Formal Complaints

AUTHORITY: 18 U.S.C. 6002; 28 U.S.C. 2461 (note); 49 U.S.C. 114, 20109, 31105, 40113–40114, 40119, 44901–44907, 46101–46107, 46109–46110, 46301, 46305, 46311, 46313–46314; Sec. 1413(i), Public Law 110–53, 121 Stat. 414 (6 U.S.C. 1142).

SOURCE: 74 FR 36039, July 21, 2009, unless otherwise noted.

Subpart A [Reserved]

Subpart B—Scope of Investigative and Enforcement Procedures

§ 1503.101 TSA requirements.

(a) The investigative and enforcement procedures in this part apply to TSA's investigation and enforcement of violations of TSA requirements.

(b) For purposes of this part, the term *TSA requirements* means the following statutory provisions and a regulation prescribed or order issued under any of those provisions:

(1) Those provisions of title 49 U.S.C. administered by the Administrator; and

(2) 46 U.S.C. chapter 701.

§ 1503.103 Terms used in this part.

In addition to the terms in § 1500.3 of this chapter, the following definitions apply in this part:

Administrative law judge or *ALJ* means an ALJ appointed pursuant to the provisions of 5 U.S.C. 3105.

Agency attorney means the Deputy Chief Counsel for Enforcement or an attorney that he or she designates. An *agency attorney* will not include—

(1) Any attorney in the Office of the Chief Counsel who advises the TSA decision maker regarding an initial decision or any appeal to the TSA decision maker; or

(2) Any attorney who is supervised in a civil penalty action by a person who provides such advice to the TSA decision maker in that action or a factually related action.

Attorney means any person who is eligible to practice law in, and is a member in good standing of the bar of, the highest court of any State, possession, territory, or Commonwealth of the United States, or of the District of Columbia, and is not under any order suspending, enjoining, restraining, disbarring, or otherwise restricting him or her in the practice of law.

Enforcement Investigative Report or *EIR* means a written report prepared by a TSA Inspector or other authorized agency official detailing the results of an inspection or investigation of a violation of a TSA requirement, including copies of any relevant evidence.

Mail includes regular First Class U.S. mail service, U.S. certified mail, or U.S. registered mail.

Party means the respondent or TSA.

Personal delivery includes hand-delivery or use of a contract or express messenger service, including an overnight express courier service. *Personal delivery* does not include the use of Government interoffice mail service.

Pleading means a complaint, an answer, motion and any amendment of these documents permitted under this subpart as well as any other written submission to the ALJ or a party during the course of the hearing proceedings.

Properly addressed means a document that shows an address contained in agency records, a residential, business, or other address submitted by a person on any document provided under this part, or any other address obtained by other reasonable and available means.

Public transportation agency means a publicly owned operator of public transportation eligible to receive Federal assistance under 49 U.S.C. chapter 53.

Respondent means the person named in a Notice of Proposed Civil Penalty, a Final Notice of Proposed Civil Penalty and Order, or a complaint.

TSA decision maker means the Administrator, acting in the capacity of the decision maker on appeal, or any person to whom the Administrator has delegated the Administrator's decision-making authority in a civil penalty action. As used in this part, the *TSA decision maker* is the official authorized to issue a final decision and order of the Administrator in a civil penalty action.

Subpart C—Investigative Procedures

§ 1503.201 Reports of violations.

(a) Any person who knows of a violation of a TSA requirement should report it to appropriate personnel of any TSA office.

(b) TSA will review each report made under this section, together with any other information TSA may have that is relevant to the matter reported, to determine the appropriate response, including additional investigation or administrative or legal enforcement action.

§ 1503.203 Investigations.

(a) *General.* The Administrator, or a designated official, may conduct investigations, hold hearings, issue subpoenas, require the production of relevant documents, records, and property, and take evidence and depositions.

(b) *Delegation of authority.* For the purpose of investigating alleged violations of a TSA requirement, the Administrator's authority may be exercised by the agency's various offices for matters within their respective areas for all routine investigations. When the compulsory processes of 49 U.S.C. 46104 are invoked, the Administrator's authority has been delegated to the Chief Counsel, each Deputy Chief Counsel, and in consultation with the Office of Chief Counsel, the Assistant Administrator for Security Operations, the Assistant Administrator for Transportation Sector Network Management, the Assistant Administrator for Inspections, the Assistant Administrator for Law Enforcement/Director of the Federal Air Marshal Service, each Special Agent in Charge, and each Federal Security Director.

§ 1503.205 Records, documents, and reports.

Each record, document, and report that regulations issued by the Transportation Security Administration require to be maintained, exhibited, or submitted to the Administrator may be used in any investigation conducted by the Administrator; and, except to the extent the use may be specifically limited or prohibited by the section that imposes the requirement, the records, documents, and reports may be used in any civil penalty action or other legal proceeding.

Subpart D—Non-Civil Penalty Enforcement

§ 1503.301 Warning notices and letters of correction.

(a) If TSA determines that a violation or an alleged violation of a TSA requirement does not require the assessment of a civil penalty, an appropriate official of the TSA may take administrative action in disposition of the case.

(b) An administrative action under this section does not constitute a formal adjudication of the matter, and may be taken by issuing the alleged violator—

(1) A ''Warning Notice'' that recites available facts and information about the incident or condition and indicates that it may have been a violation; or

(2) A ''Letter of Correction'' that confirms the TSA decision in the matter and states the necessary corrective action the alleged violator has taken or agrees to take. If the agreed corrective action is not fully completed, legal enforcement action may be taken.

(c) The issuance of a Warning Notice or Letter of Correction is not subject to appeal under this part.

(d) In the case of a public transportation agency that is determined to be in violation of a TSA requirement, an appropriate TSA official will seek correction of the violation through a written ''Notice of Noncompliance'' to the public transportation agency giving the public transportation agency reasonable opportunity to correct the violation or propose an alternative means of compliance acceptable to TSA.

(e) TSA will not take legal enforcement action against a public transportation agency under subpart E unless it has provided the Notice of Noncompliance described in paragraph (d) of this section and the public transportation agency fails to correct the violation or propose an alternative means of compliance acceptable to TSA within the timeframe provided in the notice.

(f) TSA will not initiate civil enforcement action for violations of administrative and procedural requirements pertaining to the application for, and the expenditure of, funds awarded pursuant to transportation security grant programs under Public Law 110–53.

Subpart E—Assessment of Civil Penalties by TSA

§ 1503.401 Maximum penalty amounts.

(a) *General.* TSA may assess civil penalties not exceeding the following amounts against a person for the violation of a TSA requirement.

(b) *In general.* Except as provided in paragraph (c) of this section, in the case of violation of title 49 U.S.C. or 46 U.S.C. chapter 701, or a regulation prescribed or order issued under any of those provisions, TSA may impose a civil penalty in the following amounts:

(1) $10,000 per violation, up to a total of $50,000 per civil penalty action, in

the case of an individual or small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); and

(2) $10,000 per violation, up to a total of $400,000 per civil penalty action, in the case of any other person.

(c) *Certain aviation related violations.* In the case of a violation of 49 U.S.C. chapter 449 (except sections 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909), or 49 U.S.C. 46302 or 46303, or a regulation prescribed or order issued under any of those provisions, TSA may impose a civil penalty in the following amounts:

(1) $10,000 per violation, up to a total of $50,000 per civil penalty action, in the case of an individual (except an airman serving as an airman), any person not operating an aircraft for the transportation of passengers or property for compensation, or a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632).

(2) $25,000 per violation, up to a total of $400,000 per civil penalty action, in the case of a person operating an aircraft for the transportation of passengers or property for compensation (except an individual serving as an airman).

(d) *Inflation adjustment.* TSA may adjust the maximum civil penalty amounts in conformity with the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. 2461 (note). Minimum and maximum civil penalties within the jurisdiction of TSA are adjusted for inflation as follows:

TABLE 1—MINIMUM AND MAXIMUM CIVIL PENALTIES—ADJUSTED FOR INFLATION, EFFECTIVE DECEMBER 12, 2003 TO AUGUST 20, 2009

United States Code citation	Civil penalty description	Minimum penalty	Adjusted minimum penalty	Maximum penalty amount when last set or adjusted pursuant to law	Maximum penalty amount
49 U.S.C. 46301(a)(1), (4)	Violation of 49 U.S.C. ch. 449 (except secs. 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909), or 49 U.S.C. 46302 or 46303, a regulation prescribed, or order issued thereunder by a person operating an aircraft for the transportation of passengers or property for compensation.	N/A	N/A	$25,000 per violation, reset 12/12/2003.	$25,000 per violation.
49 U.S.C. 46301(a)(1), (4)	Violation of 49 U.S.C. ch. 449 (except secs. 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909), or 49 U.S.C. 46302 or 46303, a regulation prescribed, or order issued thereunder by an individual (except an airman serving as an airman), any person not operating an aircraft for the transportation of passengers or property for compensation, or a small business concern.	N/A	N/A	$10,000 per violation, reset 12/12/2003.	$10,000 per violation.

TABLE 2—MINIMUM AND MAXIMUM CIVIL PENALTIES—ADJUSTED FOR INFLATION, EFFECTIVE AUGUST 20, 2009

United States Code Citation	Civil penalty description	Minimum penalty	Adjusted minimum penalty	Maximum penalty amount when last set or adjusted pursuant to law	Maximum penalty amount
49 U.S.C. 46301(a)(1), (4)	Violation of 49 U.S.C. ch. 449 (except secs. 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909), or 49 U.S.C. 46302 or 46303, a regulation prescribed, or order issued thereunder by a person operating an aircraft for the transportation of passengers or property for compensation.	N/A	N/A	$25,000 per violation, reset 12/12/2003.	$27,500 per violation.
49 U.S.C. 46301(a)(1), (4)	Violation of 49 U.S.C. ch. 449 (except secs. 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909), or 49 U.S.C. 46302 or 46303, a regulation prescribed, or order issued thereunder by an individual (except an airman serving as an airman), any person not operating an aircraft for the transportation of passengers or property for compensation, or a small business concern.	N/A	N/A	$10,000 per violation, reset 12/12/2003.	$11,000 per violation.
49 U.S.C. 114(v)	Violation of any other provision of title 49 U.S.C. or of 46 U.S.C. ch. 701, a regulation prescribed, or order issued under thereunder.	N/A	N/A	NA	$10,000 per violation.

§ 1503.403 Delegation of authority.

The Administrator delegates the following authority to the Chief Counsel and the Deputy Chief Counsel for Enforcement, which authority may be redelegated as necessary:

(a) To initiate and assess civil penalties under 49 U.S.C. 114 and 46301 and this subpart for a violation a TSA requirement;

(b) To compromise civil penalties initiated under this subpart; and

(c) To refer cases to the Attorney General of the United States, or the delegate of the Attorney General, for the collection of civil penalties.

§ 1503.405 Injunctions.

Whenever it is determined that a person has engaged, or is about to engage, in any act or practice constituting a violation of a TSA requirement, the Chief Counsel or the Deputy Chief Counsel for Enforcement may request the Attorney General of the United States, or the delegate of the Attorney General, to bring an action in the appropriate United States district court for such relief as is necessary or appropriate, including mandatory or prohibitive injunctive relief, interim equitable relief, and punitive damages, as provided by 49 U.S.C. 114 and 46107.

§ 1503.407 Military personnel.

If a report made under this part indicates that, while performing official duties, a member of the Armed Forces, or a civilian employee of the Department of Defense who is subject to the Uniform Code of Military Justice (10 U.S.C. chapter 47), has violated a TSA requirement, an agency official will send a copy of the report to the appropriate military authority for such disciplinary action as that authority considers appropriate and a report to the Administrator thereon.

§ 1503.409 Service of documents.

(a) *General.* This section governs service of documents required to be made under this part.

(b) *Type of service.* A person may serve documents by:

(1) Personal delivery;

(2) Mail, or

(3) Electronic mail or facsimile transmission, if consented to in writing by the person served, except that such service is not effective if the party making service receives credible information indicating that the attempted service did not reach the person to be served.

(c) If a party serves a pleading on another party during the course of hearing proceedings by electronic mail or facsimile transmission, the party making service must file with the Enforcement Docket Clerk a copy of the consent of the receiving party to accept such method of service.

(d) *Date of service.* The date of service will be:

(1) The date of personal delivery.

(2) If mailed, the mailing date stated on the certificate of service, the date shown on the postmark if there is no certificate of service, or other mailing date shown by other evidence if there is no certificate of service or postmark.

(3) If sent by electronic mail or facsimile transmission, the date of transmission.

(e) *Valid service.* A document served by mail or personal delivery that was properly addressed, was sent in accordance with this part, and that was returned, that was not claimed, or that was refused, is deemed to have been served in accordance with this part. The service will be considered valid as of the date and the time that the document was deposited with a contract or express messenger, the document was mailed, or personal delivery of the document was attempted and refused.

(f) *Presumption of service.* There will be a presumption of service where a party or a person, who customarily receives mail, or receives it in the ordinary course of business, at either the person's residence or the person's principal place of business, acknowledges receipt of the document.

(g) *Additional time after service by mail.* Whenever a party has a right or a duty to act or to make any response within a prescribed period after service by mail, or on a date certain after service by mail, 5 days will be added to the prescribed period.

(h) *Service of documents filed with the Enforcement Docket.* A person must serve a copy of any document filed

with the Enforcement Docket on each party and the ALJ or the chief ALJ if no judge has been assigned to the proceeding at the time of filing. Service on a party's attorney of record or a party's designated representative is service on the party.

(i) *Certificate of service.* Each party must attach a certificate of service to any document tendered for filing with the Enforcement Docket Clerk. A certificate of service must consist of a statement, dated and signed by the person who effected service, of the name(s) of the person(s) served, and the method by which each person was served and the date that the service was made.

(j) *Service by the ALJ.* The ALJ must serve a copy of each document he or she issues including, but not limited to, notices of pre-hearing conferences and hearings, rulings on motions, decisions, and orders, upon each party to the proceedings.

§ 1503.411 Computation of time.

(a) This section applies to any period of time prescribed or allowed by this part, or by notice or order of an ALJ.

(b) The date of an act, event, or default, after which a designated time period begins to run, is not included in a computation of time under this subpart.

(c) The last day of a time period is included in a computation of time unless it is a Saturday, Sunday, a legal holiday, or a day on which the enforcement docket is officially closed. If the last day of the time period is a Saturday, Sunday, legal holiday, or a day on which the enforcement docket is officially closed, the time period runs until the end of the next day that is not a Saturday, Sunday, legal holiday, or a day on which the enforcement docket is officially closed.

§ 1503.413 Notice of Proposed Civil Penalty.

(a) *Issuance.* TSA may initiate a civil penalty action under this section by serving a Notice of Proposed Civil Penalty on the person charged with a violation of a TSA requirement. TSA will serve the Notice of Proposed Civil Penalty on the individual charged with a violation or on the president of the corporation or company charged with a violation, or other representative or employee previously identified in writing to TSA as designated to receive such service. A corporation or company may designate in writing to TSA another person to receive service of any subsequent documents in that civil penalty action.

(b) *Contents.* The Notice of Proposed Civil Penalty contains a statement of the facts alleged, the statute, regulation, or order allegedly violated, the amount of the proposed civil penalty, and a certificate of service.

(c) *Response.* Not later than 30 days after receipt of the Notice of Proposed Civil Penalty, the person charged with a violation may take one, and only one, of the following options.

(1) Submit a certified check or money order in the amount of the proposed civil penalty made payable to Transportation Security Administration, at the address specified in the Notice of Proposed Civil Penalty, or make payment electronically through *http://www.pay.gov*.

(2) Submit to the agency attorney who issued the Notice of Proposed Civil Penalty one of the following:

(i) A written request that TSA issue an Order Assessing Civil Penalty in the amount stated in the Notice of Proposed Civil Penalty without further notice, in which case the person waives the right to request a Formal Hearing, and payment is due within 30 days of receipt of the Order.

(ii) Written information and other evidence, including documents and witness statements, demonstrating that a violation of the regulations did not occur as alleged, or that the proposed penalty is not warranted by the circumstances.

(iii) A written request to reduce the proposed civil penalty, the amount of requested reduction, together with any documents supporting a reduction of the proposed civil penalty, which reflect a current financial inability to pay or records showing that payment of the proposed civil penalty would prevent the person from continuing in business.

(iv) A written request for an Informal Conference, at a date to be determined by the agency attorney, to discuss the matter with the agency attorney and

to submit supporting evidence and information to the agency attorney before the date of the Informal Conference.

(3) Submit to the agency attorney and to TSA's Enforcement Docket Clerk a written request for a Formal Hearing before an ALJ in accordance with subpart G of this part. TSA's Enforcement Docket Clerk is currently located at the United States Coast Guard (USCG) ALJ Docketing Center, 40 S. Gay Street, Room 412, Baltimore, Maryland 21202–4022. If this location changes, TSA will provide notice of the change by notice in the FEDERAL REGISTER.

§ 1503.415 Request for portions of the enforcement investigative report (EIR).

(a) Upon receipt of a Notice of Proposed Civil Penalty, a person charged with a violation of a TSA requirement, or a representative designated in writing by that person, may request from the agency attorney who issued the Notice of Proposed Civil Penalty portions of the relevant EIR that are not privileged (*e.g.*, under the deliberative process, attorney work-product, or attorney-client privileges). This information will be provided for the sole purpose of providing the information necessary to prepare a response to the allegations contained in the Notice of Proposed Civil Penalty. Sensitive Security Information (SSI) contained in the EIR may be released pursuant to 49 CFR part 1520. Information released under this section is not produced under the Freedom of Information Act.

(b) Any person not listed in paragraph (a) of this section that is interested in obtaining a copy of the EIR must submit a FOIA request pursuant to 5 U.S.C. 552, *et seq.*, 49 CFR part 7, and any applicable DHS regulations. Portions of the EIR may be exempt from disclosure pursuant to FOIA.

§ 1503.417 Final Notice of Proposed Civil Penalty and Order.

(a) *Issuance.* TSA may issue a Final Notice of Proposed Civil Penalty and Order (''Final Notice and Order'') to a person charged with a violation in the following circumstances:

(1) The person has failed to respond to a Notice of Proposed Civil Penalty within 30 days after receipt of that notice.

(2) The person requested an Informal Conference under § 1503.413(c)(2), but failed to attend the conference or continuation of the conference or provide the agency attorney with a written request showing good cause for rescheduling of the informal conference to a specified alternate date.

(3) The parties have participated in an Informal Conference or other informal proceedings as provided in § 1503.413(c)(2) and the parties have not agreed to compromise the action or the agency attorney has not agreed to withdraw the notice of proposed civil penalty.

(b) *Contents.* The Final Notice and Order will contain a statement of the facts alleged, the law allegedly violated by the respondent, and the amount of the proposed civil penalty. The Final Notice and Order may reflect a modified allegation or proposed civil penalty as a result of information submitted to the agency attorney during the informal proceedings held under § 1503.413(c)(2).

§ 1503.419 Order Assessing Civil Penalty.

(a) *Issuance pursuant to a settlement.* TSA will issue an Order Assessing Civil Penalty if the parties have participated in an Informal Conference or other informal proceedings as provided in § 1503.413(c)(2) and agreed to a civil penalty amount in compromise of the matter, in which case the person waives the right to request a formal hearing, and payment is due within 30 days of receipt of the Order.

(b) *Automatic issuance.* A Final Notice and Order automatically converts to an Order Assessing Civil Penalty if—

(1) The person charged with a violation submits a certified check or money order in the amount reflected in the Final Notice and Order to Transportation Security Administration, to the address specified in the Final Notice and Order, or makes such payment electronically through *http://www.pay.gov*; or

(2) The person fails to respond to the Final Notice and Order or request a

formal hearing within 15 days after receipt of that notice.

§ 1503.421 Streamlined civil penalty procedures for certain security violations.

(a) *Notice of violation.* TSA, at the agency's discretion, may initiate a civil penalty action through issuance of a Notice of Violation for violations described in the section and as otherwise provided by the Administrator. TSA may serve a Notice of Violation on an individual who violates a TSA requirement by presenting a weapon, explosive, or incendiary for screening at an airport or in checked baggage, where the amount of the proposed civil penalty is less than $5,000.

(b) *Contents.* A Notice of Violation contains a statement of the charges, the amount of the proposed civil penalty, and an offer to settle the matter for a lesser specified penalty amount.

(c) *Response.* Not later than 30 days after receipt of the Notice of Violation, the individual charged with a violation must respond to TSA by taking one, and only one, of the following options.

(1) Submit a certified check or money order for the lesser specified penalty amount in the Notice of Violation, made payable to Transportation Security Administration and sent to the address specified in the Notice of Violation, or make such payment electronically through *http://www.pay.gov*.

(2) Submit to the office identified in the Notice of Violation one of the following:

(i) Written information and other evidence, including documents and witness statements, demonstrating that a violation of the regulations did not occur as alleged, or that the proposed penalty is not warranted by the circumstances.

(ii) A written request to reduce the proposed civil penalty, the amount of requested reduction, together with any documents supporting a reduction of the proposed civil penalty, which reflect a current financial inability to pay or records showing that payment of the proposed civil penalty would prevent the person from continuing in business.

(iii) A written request for an Informal Conference, at a date to be determined by an agency official, to discuss the matter with the agency official and to submit supporting evidence and information to the agency official before the date of the Informal Conference.

(3) Submit to the office identified in the Notice of Violation and to TSA's Enforcement Docket Clerk a written request for a formal hearing before an ALJ in accordance with subpart G. A request for a formal hearing before an ALJ must be submitted to the address provided in § 1503.413(c)(3).

(d) *Final Notice of Violation and Civil Penalty Assessment Order.* TSA may issue a Final Notice of Violation and Civil Penalty Assessment Order (''Final Notice and Order'') to the recipient of a Notice of Violation in the following circumstances:

(1) The individual has failed to respond to a Notice of Violation within 30 days after receipt of that notice.

(2) The individual requested an Informal Conference under § 1503.421(c)(2)(iii) but failed to attend the conference or continuation of the conference or provide the agency official with a written request showing good cause for rescheduling the informal conference to a specified alternate date.

(3) The parties have participated in an Informal Conference or other informal proceedings as provided in § 1503.421(c)(2) and the parties have not agreed to compromise the action or the agency official has not agreed to withdraw the Notice of Violation.

(e) *Order Assessing Civil Penalty.* A Final Notice and Order automatically converts to an Order Assessing Civil Penalty if—

(1) The individual charged with a violation submits a certified check or money order in the amount reflected in the Final Notice and Order to Transportation Security Administration at the address specified in the Final Notice and Order, or makes such payment electronically through *http://www.pay.gov*; or

(2) The individual fails to respond to the Final Notice and Order or request a formal hearing within 15 days after receipt of that notice.

(f) *Delegation of authority.* The authority of the Administrator, under 49 U.S.C. 46301, to initiate, negotiate, and settle civil penalty actions under this

section is delegated to the Assistant Administrator for Security Operations. This authority may be further delegated.

§ 1503.423 Consent orders.

(a) *Issuance.* At any time before the issuance of an Order Assessing Civil Penalty under this subpart, an agency attorney and a person subject to a Notice of Proposed Civil Penalty, or an agency official and a person subject to a Notice of Violation, may agree to dispose of the case by the issuance of a consent order by TSA.

(b) *Contents.* A consent order contains the following:

(1) An admission of all jurisdictional facts.

(2) An admission of agreed-upon allegations.

(3) A statement of the law violated.

(4) A finding of violation.

(5) An express waiver of the right to further procedural steps and of all rights to administrative and judicial review.

§ 1503.425 Compromise orders.

(a) *Issuance.* At any time before the issuance of an Order Assessing Civil Penalty under this subpart, an agency attorney and a person subject to a Notice of Proposed Civil Penalty, or an agency official and a person subject to a Notice of Violation, may agree to dispose of the case by the issuance of a compromise order by TSA.

(b) *Contents.* A compromise order contains the following:

(1) All jurisdictional facts.

(2) All allegations.

(3) A statement that the person agrees to pay the civil penalty specified.

(4) A statement that TSA makes no finding of a violation.

(5) A statement that the compromise order will not be used as evidence of a prior violation in any subsequent civil penalty proceeding.

§ 1503.427 Request for a formal hearing.

(a) *General.* Any respondent may request a formal hearing, pursuant to § 1503.413(c)(3) or § 1503.421(c)(3), to be conducted in accordance with the procedures in subpart G of this part. The filing of a request for a formal hearing does not guarantee a person an opportunity to appear before an ALJ in person, because the ALJ may issue an initial decision or dispositive order resolving the case prior to the commencement of the formal hearing.

(b) *Form.* The person submitting a request for hearing must date and sign the request, and must include his or her current address. The request for hearing must be typewritten or legibly handwritten.

(c) *Submission of request.* A person requesting a hearing must file a written request for a hearing with the Enforcement Docket Clerk in accordance with § 1503.429 and must serve a copy of the request on the agency attorney or other agency official who issued the Notice of Proposed Civil Penalty, or Notice of Violation, as applicable, and any other party, in accordance with § 1503.429.

§ 1503.429 Filing of documents with the Enforcement Docket Clerk.

(a) *General.* This section governs filing of documents with the Enforcement Docket Clerk when required under this part.

(b) *Type of service.* A person must file a document with the Enforcement Docket Clerk by delivering two copies of the document as follows:

(1) By personal delivery or mail, to United States Coast Guard (USCG) ALJ Docketing Center, ATTN: Enforcement Docket Clerk, at the address specified in § 1503.413(c)(3).

(2) By electronic mail, to *ALJdocket@ALJBalt.USCG.MIL.* If this e-mail address changes, TSA will provide notice of the change by notice in the FEDERAL REGISTER.

(3) By facsimile transmission, to 410–962–1746. If this number changes, TSA will provide notice of the change by notice in the FEDERAL REGISTER.

(c) *Contents.* Unless otherwise specified in this part, each document must contain a short, plain statement of the facts supporting the person's position and a brief statement of the action requested in the document. Each document must be typewritten or legibly handwritten.

(d) *Date of filing.* The date of filing will be as follows:

(1) The date of personal delivery.

(2) If mailed, the mailing date stated on the certificate of service, the date shown on the postmark if there is no certificate of service, or other mailing date shown by other evidence if there is no certificate of service or postmark.

(3) If sent by electronic mail or facsimile transmission, the date of transmission.

(e) *Service of documents filed with the Enforcement Docket.* A person must serve a copy of any document filed with the Enforcement Docket on each party and the ALJ or the chief ALJ if no judge has been assigned to the proceeding at the time of filing. Service on a party's attorney of record or a party's designated representative is service on the party.

§ 1503.431 Certification of documents.

(a) *General.* This section governs each document tendered for filing with the Enforcement Docket Clerk under this part.

(b) *Signature required.* The attorney of record, the party, or the party's representative must sign each document tendered for filing with the Enforcement Docket Clerk, or served on the ALJ, the TSA decision maker on appeal, or each party.

(c) *Effect of signing a document.* By signing a document, the attorney of record, the party, or the party's representative certifies that he or she has read the document and, based on reasonable inquiry and to the best of that person's knowledge, information, and belief, the document is—

(1) Consistent with the rules in this part;

(2) Warranted by existing law or that a good faith and nonfrivolous argument exists for extension, modification, or reversal of existing law;

(3) Not unreasonable or unduly burdensome or expensive, not made to harass any person, not made to cause unnecessary delay, not made to cause needless increase in the cost of the proceedings, or for any other improper purpose; and

(4) Supported by evidence, and any denials of factual contentions are warranted on the evidence.

(d) *Sanctions.* On motion of a party, if the ALJ or TSA decision maker finds that any attorney of record, the party, or the party's representative has signed a document in violation of this section, the ALJ or the TSA decision maker, as appropriate, will do the following:

(1) Strike the pleading signed in violation of this section.

(2) Strike the request for discovery or the discovery response signed in violation of this section and preclude further discovery by the party.

(3) Deny the motion or request signed in violation of this section.

(4) Exclude the document signed in violation of this section from the record.

(5) Dismiss the interlocutory appeal and preclude further appeal on that issue by the party who filed the appeal until an initial decision has been entered on the record.

(6) Dismiss the appeal of the ALJ's initial decision to the TSA decision maker.

Subpart F [Reserved]

Subpart G—Rules of Practice in TSA Civil Penalty Actions

§ 1503.601 Applicability.

(a) This subpart applies to a civil penalty action in which the requirements of paragraphs (a)(1) through (a)(3) of this section are satisfied.

(1) There is an alleged violation of a TSA requirement.

(2) The amount in controversy does not exceed—

(i) $50,000 if the violation was committed by an individual or a small business concern;

(ii) $400,000 if the violation was committed by any other person.

(3) The person charged with the violation has requested a hearing in accordance with § 1503.427 of this part.

(b) This subpart does not apply to the adjudication of the validity of any TSA rule or other requirement under the U.S. Constitution, the Administrative Procedure Act, or any other law.

§ 1503.603 Separation of functions.

(a) Civil penalty proceedings, including hearings, will be prosecuted only by an agency attorney, except to the

extent another agency official is permitted to issue and prosecute civil penalties under §1503.421 of this part.

(b) An agency employee engaged in the performance of investigative or prosecutorial functions in a civil penalty action must not, in that case or a factually related case, participate or give advice in a decision by the ALJ or by the TSA decision maker on appeal, except as counsel or a witness in the public proceedings.

(c) The Chief Counsel or an agency attorney not covered by paragraph (b) of this section will advise the TSA decision maker regarding an initial decision or any appeal of a civil penalty action to the TSA decision maker.

§1503.605 Appearances and rights of parties.

(a) Any party may appear and be heard in person.

(b) Any party may be accompanied, represented, or advised by an attorney or representative designated by the party and may be examined by that attorney or representative in any proceeding governed by this subpart. An attorney or representative who represents a respondent and has not previously filed a pleading in the matter must file a notice of appearance in the action, in the manner provided in §1503.429, and must serve a copy of the notice of appearance on each party, in the manner provided in §1503.409, before participating in any proceeding governed by this subpart. The attorney or representative must include the name, address, and telephone number of the attorney or representative in the notice of appearance.

§1503.607 Administrative law judges.

(a) *Powers of an ALJ.* In accordance with the rules of this subpart, an ALJ may:

(1) Give notice of, and hold, prehearing conferences and hearings.

(2) Issue scheduling orders and other appropriate orders regarding discovery or other matters that come before him or her consistent with the rules of this subpart.

(3) Administer oaths and affirmations.

(4) Issue subpoenas authorized by law.

(5) Rule on offers of proof.

(6) Receive relevant and material evidence.

(7) Regulate the course of the hearing in accordance with the rules of this subpart.

(8) Hold conferences to settle or to simplify the issues on his or her own motion or by consent of the parties.

(9) Rule on procedural motions and requests.

(10) Make findings of fact and conclusions of law, and issue an initial decision.

(11) Strike unsigned documents unless omission of the signature is corrected promptly after being called to the attention of the attorney or party.

(12) Order payment of witness fees in accordance with §1503.649.

(b) *Limitations on the power of the ALJ.* (1) The ALJ may not:

(i) Issue an order of contempt.

(ii) Award costs to any party.

(iii) Impose any sanction not specified in this subpart.

(iv) Adopt or follow a standard of proof or procedure contrary to that set forth in this subpart.

(v) Decide issues involving the validity of a TSA regulation, order, or other requirement under the U.S. Constitution, the Administrative Procedure Act, or other law.

(2) If the ALJ imposes any sanction not specified in this subpart, a party may file an interlocutory appeal of right pursuant to §1503.631(c)(3).

(3) This section does not preclude an ALJ from issuing an order that bars a person from a specific proceeding based on a finding of obstreperous or disruptive behavior in that specific proceeding.

(c) *Disqualification.* The ALJ may disqualify himself or herself at any time. A party may file a motion, pursuant to §1503.629(f)(6), requesting that an ALJ be disqualified from the proceedings.

§1503.609 Complaint.

(a) *Filing.* The agency attorney must file the complaint with the Enforcement Docket Clerk in accordance with §1503.429, or may file a written motion pursuant to §1503.629(f)(2)(i) instead of filing a complaint, not later than 30

days after receipt by the agency attorney of a request for hearing. The agency attorney should suggest a location for the hearing when filing the complaint.

(b) *Contents.* A complaint must set forth the facts alleged, any statute, regulation, or order allegedly violated by the respondent, and the proposed civil penalty in sufficient detail to provide notice of any factual or legal allegation and proposed civil penalty.

§ 1503.611 Answer.

(a) *Filing.* A respondent must file a written answer to the complaint in accordance with §1503.429, or may file a written motion pursuant to §1503.629(f)(1)–(4) instead of filing an answer, not later than 30 days after service of the complaint. Subject to paragraph (c) of this section, the answer may be in the form of a letter, but must be dated and signed by the person responding to the complaint. An answer may be typewritten or may be legibly handwritten. The person filing an answer should suggest a location for the hearing when filing the answer.

(b) *Contents.* An answer must specifically state any affirmative defense that the respondent intends to assert at the hearing. A person filing an answer may include a brief statement of any relief requested in the answer.

(c) *Specific denial of allegations required.* A person filing an answer must admit, deny, or state that the person is without sufficient knowledge or information to admit or deny, each numbered paragraph of the complaint. Any statement or allegation contained in the complaint that is not specifically denied in the answer may be deemed an admission of the truth of that allegation. A general denial of the complaint is deemed a failure to file an answer.

(d) *Failure to file answer.* A person's failure to file an answer without good cause, as determined by the ALJ, will be deemed an admission of the truth of each allegation contained in the complaint.

§ 1503.613 Consolidation and separation of cases.

(a) *Consolidation.* If two or more actions involve common questions of law or fact, the Chief Administrative Law Judge may do the following:

(1) Order a joint hearing or trial on any or all such questions.

(2) Order the consolidation of such actions.

(3) Otherwise make such orders concerning the proceedings as may tend to avoid unnecessary costs or delay.

(b) *Consolidation shall not affect the applicability of this part.* Consolidation of two or more actions that individually meet the jurisdictional amounts set forth in §1503.601(a)(2) shall not cause the resulting consolidated action to come under the exclusive jurisdiction of the district courts of the United States as specified in 49 U.S.C. 46301(d)(4)(A).

(c) *Separate trials.* The Chief Administrative Law Judge, in furtherance of convenience or to avoid prejudice, or when separate trials will be conducive to expedition and economy, may order a separate trial of any claim, or of any separate issue, or any number of claims or issues.

§ 1503.615 Notice of hearing.

(a) *Notice.* The ALJ must give each party at least 60 days notice of the date, time, and location of the hearing. With the consent of the ALJ, the parties may agree to hold the hearing on an earlier date than the date specified in the notice of hearing.

(b) *Date, time, and location of the hearing.* The ALJ to whom the proceedings have been assigned must set a reasonable date, time, and location for the hearing. The ALJ must consider the need for discovery and any joint procedural or discovery schedule submitted by the parties when determining the hearing date. The ALJ must give due regard to the convenience of the parties, the location where the majority of the witnesses reside or work, and whether the location is served by a scheduled air carrier.

§ 1503.617 Extension of time.

(a) *Oral requests.* The parties may agree to extend for a reasonable period the time for filing a document under this subpart. If the parties agree, the ALJ must grant one extension of time to each party. The party seeking the extension of time must submit a draft

order to the ALJ to be signed by the ALJ and filed with the Enforcement Docket Clerk. The ALJ may grant additional oral requests for an extension of time where the parties agree to the extension.

(b) *Written motion.* A party must file a written motion for an extension of time not later than 7 days before the document is due unless the party shows good cause for the late filing. The ALJ may grant the extension of time if the party shows good cause.

(c) *Request for continuance of hearing.* Either party may request in writing a continuance of the date of a hearing, for good cause shown, no later than seven days before the scheduled date of the hearing. Good cause does not include a scheduling conflict involving the parties or their attorneys which by due diligence could have been foreseen.

(d) *Failure to rule.* If the ALJ fails to rule on a written motion for an extension of time by the date the document was due, the motion for an extension of time is deemed granted for no more than 20 days after the original date the document was to be filed. If the ALJ fails to rule on a request for continuance by the scheduled hearing date, the request is deemed granted for no more than 10 days after the scheduled hearing date.

§ 1503.619 Intervention.

(a) A person may file a motion for leave to intervene as a party in a civil penalty action. The person must file a motion for leave to intervene not later than 10 days before the hearing unless the person shows good cause for the late filing.

(b) If the ALJ finds that intervention will not unduly broaden the issues or delay the proceedings, the ALJ may grant a motion for leave to intervene if the person will be bound by any order or decision entered in the action or the person has a property, financial, or other legitimate interest that may not be addressed adequately by the parties. The ALJ may determine the extent to which an intervenor may participate in the proceedings.

§ 1503.621 Amendment of pleadings.

(a) *Filing and service.* A party must file the amendment with the Enforcement Docket Clerk and must serve a copy of the amendment on the ALJ and all parties to the proceeding.

(b) *Time.* A party must file an amendment to a complaint or an answer within the following:

(1) Not later than 15 days before the scheduled date of a hearing, a party may amend a complaint or an answer without the consent of the ALJ.

(2) Less than 15 days before the scheduled date of a hearing, the ALJ may allow amendment of a complaint or an answer only for good cause shown in a motion to amend.

(c) *Responses.* The ALJ must allow a reasonable time, but not more than 20 days from the date of filing, for other parties to respond if an amendment to a complaint, answer, or other pleading has been filed with the ALJ.

§ 1503.623 Withdrawal of complaint or request for hearing.

At any time before or during a hearing, an agency attorney may withdraw a complaint or a respondent may withdraw a request for a hearing without the consent of the ALJ. If an agency attorney withdraws the complaint or a party withdraws the request for a hearing and the answer, the ALJ must dismiss the proceedings under this subpart with prejudice, unless the withdrawing party shows good cause for dismissal without prejudice, except that a party may withdraw a request for hearing without prejudice at any time before a complaint has been filed.

§ 1503.625 Waivers.

Waivers of any rights provided by statute or regulation must be in writing or by stipulation made at a hearing and entered into the record. The parties must set forth the precise terms of the waiver and any conditions.

§ 1503.627 Joint procedural or discovery schedule.

(a) *General.* The parties may agree to submit a schedule for filing all prehearing motions, a schedule for conducting discovery in the proceedings, or a schedule that will govern all prehearing motions and discovery in the proceedings.

(b) *Form and content of schedule.* If the parties agree to a joint procedural or

discovery schedule, one of the parties must file the joint schedule with the ALJ, setting forth the dates to which the parties have agreed, and must serve a copy of the joint schedule on each party.

(1) The joint schedule may include, but need not be limited to, requests for discovery, any objections to discovery requests, responses to discovery requests to which there are no objections, submission of prehearing motions, responses to prehearing motions, exchange of exhibits to be introduced at the hearing, and a list of witnesses that may be called at the hearing.

(2) Each party must sign the original joint schedule to be filed with the Enforcement Docket Clerk.

(c) *Time.* The parties may agree to submit all prehearing motions and responses and may agree to close discovery in the proceedings under the joint schedule within a reasonable time before the date of the hearing, but not later than 15 days before the hearing.

(d) *Order establishing joint schedule.* The ALJ must approve the joint schedule filed by the parties. One party must submit a draft order establishing a joint schedule to the ALJ to be signed by the ALJ and filed with the Enforcement Docket Clerk.

(e) *Disputes.* The ALJ must resolve disputes regarding discovery or disputes regarding compliance with the joint schedule as soon as possible so that the parties may continue to comply with the joint schedule.

(f) *Sanctions for failure to comply with joint schedule.* If a party fails to comply with the ALJ's order establishing a joint schedule, the ALJ may direct that party to comply with a motion or discovery request or, limited to the extent of the party's failure to comply with a motion or discovery request, the ALJ may do the following:

(1) Strike that portion of a party's pleadings.

(2) Preclude prehearing or discovery motions by that party.

(3) Preclude admission of that portion of a party's evidence at the hearing.

(4) Preclude that portion of the testimony of that party's witnesses at the hearing.

§ 1503.629 Motions.

(a) *General.* A party applying for an order or ruling not specifically provided in this subpart must do so by motion. A party must comply with the requirements of this section when filing a motion. A party must serve a copy of each motion on each party.

(b) *Form and contents.* A party must state the relief sought by the motion and the particular grounds supporting that relief. If a party has evidence in support of a motion, the party must attach any supporting evidence, including affidavits, to the motion.

(c) *Filing of motions.* A motion made prior to the hearing must be in writing or orally on the record. Unless otherwise agreed by the parties or for good cause shown, a party must file any prehearing motion, and must serve a copy on each party, not later than 30 days before the hearing. Motions introduced during a hearing may be made orally on the record unless the ALJ directs otherwise.

(d) *Reply to motions.* Any party may file a reply, with affidavits or other evidence in support of the reply, not later than 10 days after service of a written motion on that party. When a motion is made during a hearing, the reply may be made at the hearing on the record, orally or in writing, within a reasonable time determined by the ALJ. At the discretion of the ALJ, the moving party may file a response to the reply.

(e) *Rulings on motions.* The ALJ must rule on all motions as follows:

(1) *Discovery motions.* The ALJ must resolve all pending discovery motions not later than 10 days before the hearing.

(2) *Prehearing motions.* The ALJ must resolve all pending prehearing motions not later than 7 days before the hearing. If the ALJ issues a ruling or order orally, the ALJ must serve a written copy of the ruling or order, within 3 days, on each party. In all other cases, the ALJ must issue rulings and orders in writing and must serve a copy of the ruling or order on each party.

(3) *Motions made during the hearing.* The ALJ may issue rulings and orders on motions made during the hearing orally. Oral rulings or orders on motions must be made on the record.

(f) *Specific motions.* A party may file, but is not limited to, the following motions with the Enforcement Docket Clerk:

(1) *Motion to dismiss for insufficiency.* A respondent may file a motion to dismiss the complaint for insufficiency instead of filing an answer. If the ALJ denies the motion to dismiss the complaint for insufficiency, the respondent must file an answer not later than 20 days after service of the ALJ's denial of the motion. A motion to dismiss the complaint for insufficiency must show that the complaint fails to state a violation of a TSA requirement. If the ALJ grants the motion to dismiss the complaint for insufficiency, the agency attorney may amend the complaint in accordance with § 1503.621.

(2) *Motion to dismiss.* A party may file a motion to dismiss, specifying the grounds for dismissal. If an ALJ grants a motion to dismiss in part, a party may appeal the ALJ's ruling on the motion to dismiss under § 1503.631(b).

(i) *Motion to dismiss a request for a hearing.* An agency attorney may file a motion to dismiss a request for a hearing as untimely instead of filing a complaint. If the motion to dismiss is not granted, the agency attorney must file the complaint and must serve a copy of the complaint on each party not later than 20 days after service of the ALJ's ruling or order on the motion to dismiss. If the motion to dismiss is granted and the proceedings are terminated without a hearing, the respondent may file an appeal pursuant to § 1503.657. If required by the decision on appeal, the agency attorney must file a complaint and must serve a copy of the complaint on each party not later than 30 days after service of the decision on appeal.

(ii) *Motion to dismiss a complaint.* A respondent may file a motion to dismiss a complaint instead of filing an answer, on the ground that the complaint was not timely filed or on other grounds. If the ALJ does not grant the motion to dismiss, the respondent must file an answer and must serve a copy of the answer on each party not later than 30 days after service of the ALJ's ruling or order on the motion to dismiss. If the ALJ grants the motion to dismiss and the proceedings are terminated without a hearing, the agency attorney may file an appeal pursuant to § 1503.657. If required by the decision on appeal, the respondent must file an answer and must serve a copy of the answer on each party not later than 20 days after service of the decision on appeal.

(iii) *Motion to dismiss based on settlement.* A party may file a motion to dismiss based on a mutual settlement of the parties.

(3) *Motion for more definite statement.* A party may file a motion for more definite statement of any pleading that requires a response under this subpart. A party must set forth, in detail, the indefinite or uncertain allegations contained in a complaint or response to any pleading and must submit the details that the party believes would make the allegation or response definite and certain.

(i) *Complaint.* A respondent may file a motion requesting a more definite statement of the allegations contained in the complaint instead of filing an answer. If the ALJ grants the motion, the agency attorney must supply a more definite statement not later than 15 days after service of the ruling granting the motion. If the agency attorney fails to supply a more definite statement, the ALJ must strike the allegations in the complaint to which the motion is directed. If the ALJ denies the motion, the respondent must file an answer and must serve a copy of the answer on each party not later than 20 days after service of the order of denial.

(ii) *Answer.* An agency attorney may file a motion requesting a more definite statement if an answer fails to respond clearly to the allegations in the complaint. If the ALJ grants the motion, the respondent must supply a more definite statement not later than 15 days after service of the ruling on the motion. If the respondent fails to supply a more definite statement, the ALJ must strike those statements in the answer to which the motion is directed. The respondent's failure to supply a more definite statement may be deemed an admission of unanswered allegations in the complaint.

(4) *Motion to strike.* Any party may move to strike any insufficient allegation or defense, or any redundant, immaterial, or irrelevant matter in a pleading. A party must file a motion to strike before a response is required under this subpart or, if a response is not required, not later than 10 days after service of the pleading.

(5) *Motion for decision.* A party may move for decision, regarding all or any part of the proceedings, at any time before the ALJ has issued an initial decision in the proceedings. A party may include with a motion for decision affidavits as well as any other evidence in support of the motion. The ALJ must grant a party's motion for decision if the pleadings, depositions, answers to interrogatories, admissions, affidavits, matters that the ALJ has officially noticed, or evidence introduced during the hearing show that there is no genuine issue of material fact and that the party making the motion is entitled to a decision as a matter of law. The party moving for decision has the burden of showing that there is no genuine issue of material fact.

(6) *Motion for disqualification.* A party may file the motion at any time after the ALJ has been assigned to the proceedings but must make the motion before the ALJ files an initial decision in the proceedings.

(i) *Motion and supporting affidavit.* A party must state the grounds for disqualification, including, but not limited to, personal bias, pecuniary interest, or other factors supporting disqualification, in the motion for disqualification. A party must submit an affidavit with the motion for disqualification that sets forth, in detail, the matters alleged to constitute grounds for disqualification.

(ii) *Answer.* A party must respond to the motion for disqualification not later than 5 days after service of the motion for disqualification.

(iii) *Decision on motion for disqualification.* The ALJ must render a decision on the motion for disqualification not later than 20 days after the motion has been filed. If the ALJ finds that the motion for disqualification and supporting affidavit show a basis for disqualification, the ALJ must withdraw from the proceedings immediately. If the ALJ finds that disqualification is not warranted, the ALJ must deny the motion and state the grounds for the denial on the record. If the ALJ fails to rule on a party's motion for disqualification within 20 days after the motion has been filed, the motion is deemed granted.

(iv) *Appeal.* A party may appeal the ALJ's denial of the motion for disqualification in accordance with §1503.631(b).

§1503.631 Interlocutory appeals.

(a) *General.* Unless otherwise provided in this subpart, a party may not appeal a ruling or decision of the ALJ to the TSA decision maker until the initial decision has been entered on the record. A decision or order of the TSA decision maker on the interlocutory appeal does not constitute a final order of the Administrator for the purposes of judicial appellate review under 49 U.S.C. 46110.

(b) *Interlocutory appeal for cause.* If a party files a written request for an interlocutory appeal for cause with the ALJ, or orally requests an interlocutory appeal for cause, the proceedings are stayed until the ALJ issues a decision on the request. If the ALJ grants the request, the proceedings are stayed until the TSA decision maker issues a decision on the interlocutory appeal. The ALJ must grant an interlocutory appeal for cause if a party shows that delay of the appeal would be detrimental to the public interest or would result in undue prejudice to any party.

(c) *Interlocutory appeals of right.* If a party notifies the ALJ of an interlocutory appeal of right, the proceedings are stayed until the TSA decision maker issues a decision on the interlocutory appeal. A party may file an interlocutory appeal, without the consent of the ALJ, before an initial decision has been entered in the following cases:

(1) A ruling or order by the ALJ barring a person from the proceedings.

(2) Failure of the ALJ to dismiss the proceedings in accordance with §1503.215.

(3) A ruling or order by the ALJ in violation of §1503.607(b).

(4) A ruling or order by the ALJ regarding public access to a particular docket or documents.

(d) *Procedure.* Not later than 10 days after the ALJ's decision forming the basis of an interlocutory appeal of right or not later than 10 days after the ALJ's decision granting an interlocutory appeal for cause, a party must file a notice of interlocutory appeal, with supporting documents, and the party must serve a copy of the notice and supporting documents on each party. Not later than 10 days after service of the appeal brief, a party must file a reply brief, if any, and the party must serve a copy of the reply brief on each party. The TSA decision maker must render a decision on the interlocutory appeal, on the record and as a part of the decision in the proceedings, within a reasonable time after receipt of the interlocutory appeal.

(e) *Frivolous appeals.* The TSA decision maker may reject frivolous, repetitive, or dilatory appeals, and may issue an order precluding one or more parties from making further interlocutory appeals in a proceeding in which there have been frivolous, repetitive, or dilatory interlocutory appeals.

§ 1503.633 Discovery.

(a) *Initiation of discovery.* Any party may initiate discovery described in this section, without the consent or approval of the ALJ, at any time after a complaint has been filed in the proceedings.

(b) *Methods of discovery.* The following methods of discovery are permitted under this section: depositions on oral examination or written questions of any person; written interrogatories directed to a party; requests for production of documents or tangible items to any person; and requests for admission by a party. A party is not required to file written discovery requests and responses with the ALJ or the Enforcement Docket Clerk. In the event of a discovery dispute, a party must attach a copy of these documents in support of a motion made under this section.

(c) *Service on the agency.* A party must serve each discovery request directed to the agency or any agency employee on the agency attorney of record.

(d) *Time for response to discovery requests.* Unless otherwise directed by this subpart, agreed by the parties, or by order of the ALJ, a party must respond to a request for discovery, including filing objections to a request for discovery, not later than 30 days after service of the request.

(e) *Scope of discovery.* Subject to the limits on discovery set forth in paragraph (f) of this section, a party may discover any matter that is not privileged and that is relevant to the subject matter of the proceeding. A party may discover information that relates to the claim or defense of any party including the existence, description, nature, custody, condition, and location of any document or other tangible item and the identity and location of any person having knowledge of discoverable matter. A party may discover facts known, or opinions held, by an expert who any other party expects to call to testify at the hearing. A party may not object to a discovery request on the basis that the information sought would not be admissible at the hearing if the information sought during discovery is reasonably calculated to lead to the discovery of admissible evidence.

(f) *Limiting discovery.* The ALJ must limit the frequency and extent of discovery permitted by this section if a party shows that—

(1) The information requested is cumulative or repetitious;

(2) The information requested can be obtained from another less burdensome and more convenient source;

(3) The party requesting the information has had ample opportunity to obtain the information through other discovery methods permitted under this section; or

(4) The method or scope of discovery requested by the party is unduly burdensome or expensive.

(g) *Disclosure of Sensitive Security Information (SSI).* At the request of a party, TSA may provide SSI to the party when, in the sole discretion of TSA, access to the SSI is necessary for the party to prepare a response to allegations contained the complaint. TSA may provide such information subject to such restrictions on further disclosure and such safeguarding requirements as TSA determines appropriate.

(h) *Confidential orders.* A party or person who has received a discovery request for information, other than SSI, that is related to a trade secret, confidential or sensitive material, competitive or commercial information, proprietary data, or information on research and development, may file a motion for a confidential order with the ALJ and must serve a copy of the motion for a confidential order on each party.

(1) The party or person making the motion must show that the confidential order is necessary to protect the information from disclosure to the public.

(2) If the ALJ determines that the requested material is not necessary to decide the case, the ALJ must preclude any inquiry into the matter by any party.

(3) If the ALJ determines that the requested material may be disclosed during discovery, the ALJ may order that the material may be discovered and disclosed under limited conditions or may be used only under certain terms and conditions.

(4) If the ALJ determines that the requested material is necessary to decide the case and that a confidential order is warranted, the ALJ must provide the following:

(i) An opportunity for review of the document by the parties off the record.

(ii) Procedures for excluding the information from the record.

(iii) An order that the parties must not disclose the information in any manner and the parties must not use the information in any other proceeding.

(i) *Protective orders.* A party or a person who has received a request for discovery may file a motion for protective order and must serve a copy of the motion for protective order on each party. The party or person making the motion must show that the protective order is necessary to protect the party or the person from annoyance, embarrassment, oppression, or undue burden or expense. As part of the protective order, the ALJ may do the following:

(1) Deny the discovery request.

(2) Order that discovery be conducted only on specified terms and conditions, including a designation of the time or place for discovery or a determination of the method of discovery.

(3) Limit the scope of discovery or preclude any inquiry into certain matters during discovery.

(j) *Duty to supplement or amend responses.* A party who has responded to a discovery request has a duty to supplement or amend the response, as soon as the information is known, as follows:

(1) A party must supplement or amend any response to a question requesting the identity and location of any person having knowledge of discoverable matters.

(2) A party must supplement or amend any response to a question requesting the identity of each person who will be called to testify at the hearing as an expert witness and the subject matter and substance of that witness' testimony.

(3) A party must supplement or amend any response that was incorrect when made or any response that was correct when made but is no longer correct, accurate, or complete.

(k) *Depositions.* The following rules apply to depositions taken pursuant to this section:

(1) *Form.* A deposition must be taken on the record and reduced to writing. The person being deposed must sign the deposition unless the parties agree to waive the requirement of a signature.

(2) *Administration of oaths.* Within the United States, or a territory or possession subject to the jurisdiction of the United States, a party must take a deposition before a person authorized to administer oaths by the laws of the United States or authorized by the law of the place where the examination is held. Outside the United States, a party will take a deposition in any manner allowed by the Federal Rules of Civil Procedure (28 U.S.C. App.).

(3) *Notice of deposition.* A party must serve a notice of deposition, stating the time and place of the deposition and the name and address of each person to be examined, on the person to be deposed, on the ALJ, on the Enforcement Docket Clerk, and on each party not later than 7 days before the deposition. A party may serve a notice of deposition less than 7 days before the deposition only with consent of the ALJ and for good cause shown. If a subpoena

''duces tecum'' is to be served on the person to be examined, the party must attach a copy of the subpoena duces tecum that describes the materials to be produced at the deposition to the notice of deposition.

(4) *Use of depositions.* A party may use any part or all of a deposition at a hearing authorized under this subpart only upon a showing of good cause. The deposition may be used against any party who was present or represented at the deposition or who had reasonable notice of the deposition.

(l) *Interrogatories.* A party, the party's attorney, or the party's representative may sign the party's responses to interrogatories. A party must answer each interrogatory separately and completely in writing. If a party objects to an interrogatory, the party must state the objection and the reasons for the objection. An opposing party may use any part or all of a party's responses to interrogatories at a hearing authorized under this subpart to the extent that the response is relevant, material, and not repetitious.

(1) A party must not serve more than 30 interrogatories to each other party. Each subpart of an interrogatory will be counted as a separate interrogatory.

(2) Before serving additional interrogatories on a party, a party must file a motion for leave to serve additional interrogatories on a party with the ALJ and must serve a copy on each party before serving additional interrogatories on a party. The ALJ may grant the motion only if the party shows good cause for the party's failure to inquire about the information previously and that the information cannot reasonably be obtained using less burdensome discovery methods or be obtained from other sources.

(m) *Requests for admission.* A party may serve a written request for admission of the truth of any matter within the scope of discovery under this section or the authenticity of any document described in the request. A party must set forth each request for admission separately. A party must serve copies of documents referenced in the request for admission unless the documents have been provided or are reasonably available for inspection and copying.

(1) *Time.* A party's failure to respond to a request for admission, in writing and signed by the attorney or the party, not later than 30 days after service of the request, is deemed an admission of the truth of the statement or statements contained in the request for admission. The ALJ may determine that a failure to respond to a request for admission is not deemed an admission of the truth if a party shows that the failure was due to circumstances beyond the control of the party or the party's attorney.

(2) *Response.* A party may object to a request for admission and must state the reasons for objection. A party may specifically deny the truth of the matter or describe the reasons why the party is unable to truthfully deny or admit the matter. If a party is unable to deny or admit the truth of the matter, the party must show that the party has made reasonable inquiry into the matter or that the information known to, or readily obtainable by, the party is insufficient to enable the party to admit or deny the matter. A party may admit or deny any part of the request for admission. If the ALJ determines that a response does not comply with the requirements of this rule or that the response is insufficient, the matter is deemed admitted.

(3) *Effect of admission.* Any matter admitted or deemed admitted under this section is conclusively established for the purpose of the hearing and appeal.

(n) *Motion to compel discovery.* A party may move to compel discovery if a person refuses to answer a question during a deposition, a party fails or refuses to answer an interrogatory, if a person gives an evasive or incomplete answer during a deposition or when responding to an interrogatory, or a party fails or refuses to produce documents or tangible items. During a deposition, the proponent of a question may complete the deposition or may adjourn the examination before moving to compel if a person refuses to answer.

(o) *Failure to comply with a discovery order or order to compel.* If a party fails to comply with a discovery order or an order to compel, the ALJ, limited to the extent of the party's failure to comply with the discovery order or motion to compel, may do the following:

(1) Strike that portion of a party's pleadings.

(2) Preclude prehearing or discovery motions by that party.

(3) Preclude admission of that portion of a party's evidence at the hearing.

(4) Preclude that portion of the testimony of that party's witnesses at the hearing.

§ 1503.635 Evidence.

(a) *General.* A party is entitled to present the party's case or defense by oral, documentary, or demonstrative evidence, to submit rebuttal evidence, and to conduct any cross-examination that may be required for a full and true disclosure of the facts.

(b) *Admissibility.* A party may introduce any oral, documentary, or demonstrative evidence in support of the party's case or defense. The ALJ must admit any oral, documentary, or demonstrative evidence introduced by a party, but must exclude irrelevant, immaterial, or unduly repetitious evidence.

(c) *Hearsay evidence.* Hearsay evidence is admissible in proceedings governed by this subpart. The fact that evidence submitted by a party is hearsay goes only to the weight of the evidence and does not affect its admissibility.

§ 1503.637 Standard of proof.

The ALJ may issue an initial decision or may rule in a party's favor only if the decision or ruling is supported by a preponderance of the evidence contained in the record. In order to prevail, the party with the burden of proof must prove the party's case or defense by a preponderance of the evidence.

§ 1503.639 Burden of proof.

(a) Except in the case of an affirmative defense, the burden of proof is on the agency.

(b) Except as otherwise provided by statute or rule, the proponent of a motion, request, or order has the burden of proof.

(c) A party who has asserted an affirmative defense has the burden of proving the affirmative defense.

§ 1503.641 Offer of proof.

A party whose evidence has been excluded by a ruling of the ALJ may offer the evidence for the record on appeal.

§ 1503.643 Public disclosure of evidence.

This section applies to information other than Sensitive Security Information (SSI). All release of SSI is governed by § 1503.415 and 49 CFR part 1520.

(a) The ALJ may order that any other information contained in the record be withheld from public disclosure. Any person may object to disclosure of information in the record by filing a written motion to withhold specific information with the ALJ and serving a copy of the motion on each party. The party must state the specific grounds for nondisclosure in the motion.

(b) The ALJ must grant the motion to withhold information in the record if, based on the motion and any response to the motion, the ALJ determines that disclosure would be detrimental to transportation safety, disclosure would not be in the public interest, or that the information is not otherwise required to be made available to the public.

§ 1503.645 Expert or opinion witnesses.

An employee of the agency may not be called as an expert or opinion witness, for any party other than TSA, in any proceeding governed by this subpart. An employee of a respondent may not be called by an agency attorney as an expert or opinion witness for TSA in any proceeding governed by this subpart to which the respondent is a party.

§ 1503.647 Subpoenas.

(a) *Request for subpoena.* A party may obtain a subpoena to compel the attendance of a witness at a deposition or hearing, or to require the production of documents or tangible items, from the ALJ who is assigned to the case, or, if no ALJ is assigned or the assigned law judge is unavailable, from the chief ALJ. The party must complete the subpoena, stating the title of the action and the date and time for the witness' attendance or production of documents or items. The party who obtained the

subpoena must serve the subpoena on the witness or the custodian of the documents or tangible items sought to be produced.

(b) *Motion to quash or modify the subpoena.* A party, or any person upon whom a subpoena has been served, may file a motion to quash or modify the subpoena at or before the time specified in the subpoena for compliance. The applicant must describe, in detail, the basis for the application to quash or modify the subpoena including, but not limited to, a statement that the testimony, document, or tangible evidence is not relevant to the proceeding, that the subpoena is not reasonably tailored to the scope of the proceeding, or that the subpoena is unreasonable and oppressive. A motion to quash or modify the subpoena will stay the effect of the subpoena pending a decision by the ALJ on the motion.

(c) *Enforcement of subpoena.* Upon a showing that a person has failed or refused to comply with a subpoena, a party may apply to the U.S. district court having jurisdiction to seek judicial enforcement of the subpoena in accordance with 49 U.S.C. 46104.

§ 1503.649 Witness fees.

(a) *General.* Unless otherwise authorized by the ALJ, the party who applies for a subpoena to compel the attendance of a witness at a deposition or hearing, or the party at whose request a witness appears at a deposition or hearing, must pay the witness fees described in this section.

(b) *Amount.* Except for an employee of the agency who appears at the direction of the agency, a witness who appears at a deposition or hearing is entitled to the same fees and mileage expenses as are paid to a witness in a court of the United States in comparable circumstances.

§ 1503.651 Record.

(a) *Exclusive record.* The request for hearing, complaint, answer, transcript of all testimony in the hearing, all exhibits received into evidence, and all motions, responses to motions, applications, requests, and rulings will constitute the exclusive record for decision of the proceedings and the basis for the issuance of any orders in the proceeding.

(b) *Examination and copying of record.* (1) *Generally.* Any person interested in reviewing or obtaining a copy of a record may do so only by submitting a Freedom of Information Act (FOIA) request under 5 U.S.C. 552, *et seq.*, 49 CFR part 7, and any applicable DHS regulations. Portions of the record may be exempt from disclosure pursuant to FOIA.

(2) *Docket Files or Documents Not for Public Disclosure.* (i) Only the following persons may review docket files or particular documents that are not for public disclosure:

(A) Parties to the proceedings.

(B) Their designated representatives.

(C) Persons who have a need to know as determined by the Administrator.

(ii) Those persons with permission to review these documents or docket files may view the materials at the TSA Headquarters, 601 South 12th Street, Arlington, Virginia 20598–6002. Persons with access to these records may have a copy of the records after payment of reasonable costs.

§ 1503.653 Argument before the ALJ.

(a) *Arguments during the hearing.* During the hearing, the ALJ must give the parties a reasonable opportunity to present arguments on the record supporting or opposing motions, objections, and rulings if the parties request an opportunity for argument. The ALJ may request written arguments during the hearing if the ALJ finds that submission of written arguments is necessary before the ALJ issues the ruling or order.

(b) *Final oral argument.* At the conclusion of the hearing and before the ALJ issues an initial decision in the proceedings, the parties are entitled to submit oral proposed findings of fact and conclusions of law, exceptions to rulings of the ALJ, and supporting arguments for the findings, conclusions, or exceptions. At the conclusion of the hearing, a party may waive final oral argument.

(c) *Posthearing briefs.* The ALJ may request written posthearing briefs before the ALJ issues an initial decision in the proceedings. If a party files a written posthearing brief, the party

must include proposed findings of fact and conclusions of law, exceptions to rulings of the ALJ, and supporting arguments for the findings, conclusions, or exceptions. The ALJ must give the parties a reasonable opportunity, not more than 30 days after receipt of the transcript, to prepare and submit the briefs.

§ 1503.655 Initial decision.

(a) *Contents.* The ALJ may issue an initial decision after the conclusion of the hearing or after the submission of written posthearing briefs, if so ordered. In each oral or written decision, the ALJ must include findings of fact and conclusions of law, and the grounds supporting those findings and conclusions, upon all material issues of fact, the credibility of witnesses, the applicable law, any exercise of the ALJ's discretion, the amount of any civil penalty found appropriate by the ALJ, and a discussion of the basis for any order issued in the proceedings. The ALJ is not required to provide a written explanation for rulings on objections, procedural motions, and other matters not directly relevant to the substance of the initial decision. If the ALJ refers to any previous unreported or unpublished initial decision, the ALJ must make copies of that initial decision available to all parties and the TSA decision maker.

(b) *Written decision.* At the conclusion of the hearing, the ALJ may issue the initial decision and order orally on the record. The ALJ must issue a written initial decision and order not later than 30 days after the conclusion of the hearing or submission of the last posthearing brief. The ALJ must serve a copy of any written initial decision on each party.

(c) *Order assessing civil penalty.* Unless appealed pursuant to §1503.657, the initial decision issued by the ALJ will be considered an order assessing civil penalty if the ALJ finds that an alleged violation occurred and determines that a civil penalty, in an amount found appropriate by the ALJ, is warranted.

(d) *Effect of initial decision.* An initial decision of an ALJ is persuasive authority in any other civil penalty action, unless appealed and reversed by the TSA decision maker or a court of competent jurisdiction.

§ 1503.657 Appeal from initial decision.

(a) *Notice of appeal.* Either party may appeal the initial decision, and any decision not previously appealed pursuant to §1503.631, by filing a notice of appeal with the Enforcement Docket Clerk. A party must file the notice of appeal with USCG ALJ Docketing Center, ATTN: Enforcement Docket Clerk, 40 S. Gay Street, Room 412, Baltimore, Maryland 21202–4022. A party must file the notice of appeal not later than 10 days after entry of the oral initial decision on the record or service of the written initial decision on the parties and must serve a copy of the notice of appeal on each party. Upon filing of a notice of appeal, the effectiveness of the initial decision is stayed until a final decision and order of the TSA decision maker have been entered on the record.

(b) *Issues on appeal.* A party may appeal only the following issues:

(1) Whether each finding of fact is supported by a preponderance of the evidence.

(2) Whether each conclusion of law is made in accordance with applicable law, precedent, and public policy.

(3) Whether the ALJ committed any prejudicial errors during the hearing that support the appeal.

(c) *Perfecting an appeal.* Unless otherwise agreed by the parties, a party must perfect an appeal, not later than 50 days after entry of the oral initial decision on the record or service of the written initial decision on the party, by filing an appeal brief with the Enforcement Docket Clerk.

(1) *Extension of time by agreement of the parties.* The parties may agree to extend the time for perfecting the appeal with the consent of the TSA decision maker. If the TSA decision maker grants an extension of time to perfect the appeal, the Enforcement Docket Clerk will serve a letter confirming the extension of time on each party.

(2) *Written motion for extension.* If the parties do not agree to an extension of time for perfecting an appeal, a party desiring an extension of time may file a written motion for an extension with the Enforcement Docket Clerk and

must serve a copy of the motion on each party. The TSA decision maker may grant an extension if good cause for the extension is shown in the motion.

(d) *Appeal briefs.* A party must file the appeal brief with the Enforcement Docket Clerk and must serve a copy of the appeal brief on each party.

(1) In the appeal brief, a party must set forth, in detail, the party's specific objections to the initial decision or rulings, the basis for the appeal, the reasons supporting the appeal, and the relief requested in the appeal. If, for the appeal, the party relies on evidence contained in the record for the appeal, the party must specifically refer in the appeal brief to the pertinent evidence contained in the transcript.

(2) The TSA decision maker may dismiss an appeal, on the TSA decision maker's own initiative or upon motion of any other party, where a party has filed a notice of appeal but fails to perfect the appeal by timely filing an appeal brief.

(e) *Reply brief.* Unless otherwise agreed by the parties, any party may file a reply brief not later than 35 days after the appeal brief has been served on that party. The party filing the reply brief must serve a copy of the reply brief on each party. If the party relies on evidence contained in the record for the reply, the party must specifically refer to the pertinent evidence contained in the transcript in the reply brief.

(1) *Extension of time by agreement of the parties.* The parties may agree to extend the time for filing a reply brief with the consent of the TSA decision maker. If the TSA decision maker grants an extension of time to file the reply brief, the Enforcement Docket Clerk will serve a letter confirming the extension of time on each party.

(2) *Written motion for extension.* If the parties do not agree to an extension of time for filing a reply brief, a party desiring an extension of time may file a written motion for an extension and will serve a copy of the motion on each party. The TSA decision maker may grant an extension if good cause for the extension is shown in the motion.

(f) *Other briefs.* The TSA decision maker may allow any person to submit an amicus curiae brief in an appeal of an initial decision. A party may not file more than one appeal brief or reply brief. A party may petition the TSA decision maker, in writing, for leave to file an additional brief and must serve a copy of the petition on each party. The party may not file the additional brief with the petition. The TSA decision maker may grant leave to file an additional brief if the party demonstrates good cause for allowing additional argument on the appeal. The TSA decision maker will allow a reasonable time for the party to file the additional brief.

(g) *Number of copies.* A party must file the original appeal brief or the original reply brief, and two copies of the brief, with the Enforcement Docket Clerk.

(h) *Oral argument.* The TSA decision maker has sole discretion to permit oral argument on the appeal. On the TSA decision maker's own initiative or upon written motion by any party, the TSA decision maker may find that oral argument will contribute substantially to the development of the issues on appeal and may grant the parties an opportunity for oral argument.

(i) *Waiver of objections on appeal.* If a party fails to object to any alleged error regarding the proceedings in an appeal or a reply brief, the party waives any objection to the alleged error. The TSA decision maker is not required to consider any objection in an appeal brief or any argument in the reply brief if a party's objection is based on evidence contained in the record and the party does not specifically refer to the pertinent evidence from the record in the brief.

(j) *The TSA decision maker's decision on appeal.* The TSA decision maker will review the briefs on appeal and the oral argument, if any, to determine if the ALJ committed prejudicial error in the proceedings or that the initial decision should be affirmed, modified, or reversed. The TSA decision maker may affirm, modify, or reverse the initial decision, make any necessary findings, or may remand the case for any proceedings that the TSA decision maker determines may be necessary.

(1) The TSA decision maker may raise any issue, on the TSA decision maker's own initiative, that is required

for proper disposition of the proceedings. The TSA decision maker will give the parties a reasonable opportunity to submit arguments on the new issues before making a decision on appeal. If an issue raised by the TSA decision maker requires the consideration of additional testimony or evidence, the TSA decision maker will remand the case to the ALJ for further proceedings and an initial decision related to that issue. If the TSA decision maker raises an issue that is solely an issue of law, or the issue was addressed at the hearing but was not raised by a party in the briefs on appeal, the TSA decision maker need not remand the case to the ALJ for further proceedings but has the discretion to do so.

(2) The TSA decision maker will issue the final decision and order of the Administrator on appeal in writing and will serve a copy of the decision and order on each party. Unless a petition for review is filed pursuant to §1503.659, a final decision and order of the Administrator will be considered an order assessing civil penalty if the TSA decision maker finds that an alleged violation occurred and a civil penalty is warranted.

(3) A final decision and order of the Administrator after appeal is binding precedent in any other civil penalty action unless appealed and reversed by a court of competent jurisdiction.

(4) The TSA decision maker will determine whether the decision and order of the TSA decision maker, with the ALJ's initial decision or order attached, may be released to the public, either in whole or in redacted form. In making this determination, the TSA decision maker will consider whether disclosure of any of the information in the decision and order would be detrimental to transportation security, would not be in the public interest, or should not otherwise be required to be made available to the public.

§1503.659 Petition to reconsider or modify a final decision and order of the TSA decision maker on appeal.

(a) *General.* Any party may petition the TSA decision maker to reconsider or modify a final decision and order issued by the TSA decision maker on appeal from an initial decision. A party must file a petition to reconsider or modify not later than 30 days after service of the TSA decision maker's final decision and order on appeal and must serve a copy of the petition on each party. The TSA decision maker will not reconsider or modify an initial decision and order issued by an ALJ that has not been appealed by any party to the TSA decision maker and filed with the Enforcement Docket Clerk.

(b) *Form and number of copies.* A party must file in writing a petition to reconsider or modify. The party must file the original petition with the Enforcement Docket Clerk and must serve a copy of the petition on each party.

(c) *Contents.* A party must state briefly and specifically the alleged errors in the final decision and order on appeal, the relief sought by the party, and the grounds that support the petition to reconsider or modify.

(1) If the petition is based, in whole or in part, on allegations regarding the consequences of the TSA decision maker's decision, the party must describe and support those allegations.

(2) If the petition is based, in whole or in part, on new material not previously raised in the proceedings, the party must set forth the new material and include affidavits of prospective witnesses and authenticated documents that would be introduced in support of the new material. The party must explain, in detail, why the new material was not discovered through due diligence prior to the hearing.

(d) *Repetitious and frivolous petitions.* The TSA decision maker will not consider repetitious or frivolous petitions. The TSA decision maker may summarily dismiss repetitious or frivolous petitions to reconsider or modify.

(e) *Reply petitions.* Any other party may reply to a petition to reconsider or modify, not later than 10 days after service of the petition on that party, by filing a reply with the Enforcement Docket Clerk. A party must serve a copy of the reply on each party.

(f) *Effect of filing petition.* Unless otherwise ordered by the TSA decision maker, filing a petition pursuant to this section will stay the effective date of the TSA decision maker's final decision and order on appeal.

(g) *The TSA decision maker's decision on petition.* The TSA decision maker has sole discretion to grant or deny a petition to reconsider or modify. The TSA decision maker will grant or deny a petition to reconsider or modify within a reasonable time after receipt of the petition or receipt of the reply petition, if any. The TSA decision maker may affirm, modify, or reverse the final decision and order on appeal, or may remand the case for any proceedings that the TSA decision maker determines may be necessary.

§ 1503.661 Judicial review of a final order.

For violations of a TSA requirement, a party may petition for review of a final order of the Administrator only to the courts of appeals of the United States or the United States Court of Appeals for the District of Columbia pursuant to 49 U.S.C. 46110. A party seeking judicial review of a final order must file a petition for review not later than 60 days after the final order has been served on the party.

Subpart H—Judicial Assessment of Civil Penalties

§ 1503.701 Applicability of this subpart.

(a) *Jurisdictional minimums.* This subpart applies to a civil penalty action under this part in which the total amount in controversy exceeds the following amounts.

(b) *In general.* Except as provided in paragraph (c) of this section, in the case of violation of title 49 U.S.C. or 46 U.S.C chapter 701, a regulation prescribed, or order issued under any of those provisions, the amount in controversy exceeds the following:

(1) $50,000, in the case of violation by an individual or small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632).

(2) $400,000, in the case of violation by any other person.

(c) *Certain aviation related violations.* In the case of a violation of 49 U.S. C. chapter 449 (except sections 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909), or a regulation prescribed or order issued under any of those provisions, the amount in controversy exceeds the following:

(1) $50,000, in the case of violation by an individual (except an airman serving as an airman), any person not operating an aircraft for the transportation of passengers or property for compensation, or a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632).

(2) $400,000, in the case of violation by a person operating an aircraft for the transportation of passengers or property for compensation (except an individual serving as an airman).

§ 1503.703 Civil penalty letter; referral.

(a) *Issuance.* In a civil penalty action in which the amount in controversy exceeds the amounts set forth in § 1503.701, the Administrator will send a civil penalty letter to the person charged with a violation of a TSA requirement.

(b) *Contents.* The civil penalty letter will contain a statement of the charges; the applicable law, rule, regulation, or order; the amount of civil penalty that the Administrator will accept in full settlement of the action or an offer to compromise the civil penalty.

(c) *Response.* Not later than 30 days after receipt of the civil penalty letter, the person charged with a violation may present to the agency attorney any material or information in answer to the charges, either orally or in writing, that may explain, mitigate, or deny the violation or that may show extenuating circumstances. The Administrator will consider any material or information submitted in accordance with this paragraph (c) to determine whether the person is subject to a civil penalty or to determine the amount for which the Administrator will compromise the action.

(d) *Compromise.* If the person charged with a violation offers to compromise the civil penalty action for a specific amount, that person must send payment in a form and manner acceptable to TSA for that amount to the agency, made payable to the Transportation Security Administration, or make payment electronically through *http://www.pay.gov*. The Chief Counsel or the

Deputy Chief Counsel for Civil Enforcement may accept the payment or may refuse and return the payment. If the Administrator accepts the offer to compromise, the agency will send a letter to the person charged with the violation stating that the payment is accepted in full settlement of the civil penalty action and that the matter is closed.

(e) *Referral for prosecution and collection.* If the parties cannot agree to compromise the civil penalty action or the offer to compromise is rejected and the payment submitted in compromise is returned, the Administrator may refer the civil penalty action to the United States Attorney General, or the delegate of the Attorney General, to begin proceedings in a United States district court, pursuant to the authority in 49 U.S.C. 114 or 46305 to prosecute and collect the civil penalty.

(f) The Administrator delegates to the Chief Counsel and the Deputy Chief Counsel for Enforcement the authority to carry out any function of the Administrator described in this §1503.703.

Subpart I—Formal Complaints

§1503.801 Formal complaints.

(a) Any person may file a complaint with the Administrator with respect to any act or omission by any person in contravention of 49 U.S.C., subtitle VII, part A, (except sections 44902, 44903(d), 44907(a)–(d)(1)(A), 44907(d)(1)(C)–(f), 44908, and 44909) administered by the Administrator, or a regulation prescribed or order issued under any of those provisions. This section does not apply to complaints against the Administrator or employees of the TSA acting within the scope of their employment.

(b) Complaints filed under this section must—

(1) Be submitted in writing and identified as a complaint filed for the purpose of seeking an appropriate order or other enforcement action;

(2) Be submitted to the U.S. Department of Homeland Security, Transportation Security Administration, by following the instructions to complete a ''complaint'' contact form by following the instructions on the TSA Web site, currently accessible at *http://www.tsa.gov/contact/index.shtm.*

(3) Set forth the name and address, if known, of each person who is the subject of the complaint and, with respect to each person, the specific provisions of the statute, regulation, or order that the person filing the complaint believes were violated;

(4) Contain a concise, but complete, statement of the facts relied upon to substantiate each allegation;

(5) State the name, address, and telephone number of the person filing the complaint; and

(6) Be signed by the person filing the complaint or a duly authorized representative.

(c) TSA will consider complaints that do not meet the requirements of paragraph (b) of this section as reports under §1503.1.

(d) TSA will place complaints that meet the requirements of paragraph (b) of this section in the docket and will mail a copy to each person named in the complaint.

(e) TSA will refer any complaint against a member of the Armed Forces of the United States acting in the performance of official duties to the Secretary of the Department concerned in accordance with the procedures set forth in §1503.407.

(f) The person named in the complaint must file an answer within 20 days after service of a copy of the complaint.

(g) After the complaint has been answered or after the allotted time in which to file an answer has expired, the Administrator, or a designated official, will determine if there are reasonable grounds for investigating the complaint.

(h) If the Administrator, or a designated official, determines that a complaint does not state facts that warrant an investigation or action, the Administrator or designated official may dismiss the complaint without a hearing and, if so, will provide the reason for the dismissal, in writing, to the person who filed the complaint and the person(s) named in the complaint.

(i) If the Administrator, or a designated official, determines that reasonable grounds exist, an informal investigation may be initiated. Each person named in the complaint will be advised which official has been delegated the responsibility under §1503.203 for conducting the investigation.

(j) If the investigation substantiates the allegations set forth in the complaint, a notice of proposed order may be issued or other enforcement action taken in accordance with this part.

(k) The complaint and other pleadings and official TSA records relating to the disposition of the complaint are maintained in current docket form at: U.S. Department of Homeland Security, Transportation Security Administration, Office of the Chief Counsel, TSA–2, Complaint Docket, 601 South 12th Street, Arlington, VA 20598–6002. If this location changes, TSA will give notice of the change by publishing a notice in the FEDERAL REGISTER.

(1) *Generally.* Any person interested in reviewing or obtaining a copy of a record may do so only by submitting a Freedom of Information Act (FOIA) request under 5 U.S.C. 552, *et seq.* and 49 CFR part 7. Portions of the record may be exempt from disclosure pursuant to FOIA.

(2) *Docket files or documents not for public disclosure.* (i) Only the following persons may review docket files or particular documents that are not for public disclosure:

(A) Parties to the proceedings.

(B) Representatives designated in writing by a party.

(C) Persons who have a need to know as determined by the Administrator.

(ii) Those persons with permission to review these documents or docket files may view the materials at the Complaint Docket, TSA Headquarters, Visitor Center, 601 South 12th Street, Arlington, Virginia 20598–6002, Attn: Office of Chief Counsel. If this address changes, TSA will give notice by publishing a notice in the FEDERAL REGISTER. Persons with access to these records may have a copy of the records after payment of reasonable costs.

PART 1507—PRIVACY ACT-EXEMPTIONS

Sec.
1507.1 Scope.
1507.3 Exemptions.

AUTHORITY: 49 U.S.C. 114(l)(1), 40113, 5 U.S.C. 552a(j) and (k).

SOURCE: 69 FR 35537, June 25, 2004, unless otherwise noted.

§ 1507.1 Scope.

This part implements provisions of the Privacy Act of 1974 (the Act) that permit TSA to exempt any system of records within the agency from certain requirements of the Act. The procedures governing access to, and correction of, records in a TSA system of records are set forth in 6 CFR part 5, subpart B.

§ 1507.3 Exemptions.

The following TSA systems of records are exempt from certain provisions of the Privacy Act of 1974 pursuant to 5 U.S.C. 552a(j), (k), or both, as set forth in this section. During the course of normal agency functions, exempt materials from one system of records may become part of one or more other systems of records. To the extent that any portion of system of records becomes part of another Privacy Act system of records, TSA hereby claims the same exemptions as were claimed in the original primary system of which they are a part and claims any additional exemptions in accordance with this part.

(a) *Transportation Security Enforcement Record System (DHS/TSA 001).* The Transportation Security Enforcement Record System (TSERS) (DHS/TSA 001) enables TSA to maintain a system of records related to the screening of passengers and property and they may be used to identify, review, analyze, investigate, and prosecute violations or potential violations of criminal statutes and transportation security laws. Pursuant to exemptions (j)(2), (k)(1), and (k)(2) of the Privacy Act, DHS/TSA 001 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(3), (e)(4)(G), (H), and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of TSA, as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to transportation security, law enforcement efforts, and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension, which undermines the entire system.

(2) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and reveal investigative interest on the part of TSA, as well as the recipient agency. Access to the records would permit the individual who is the subject of a record to impede the investigation and avoid detection or apprehension. Amendment of the records would interfere with ongoing investigations and law enforcement activities, and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose sensitive security information, which could be detrimental to transportation security.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of transportation security laws, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective enforcement of transportation security laws, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(4) From subsection (e)(3) (Privacy Act Statement) because disclosing the authority, purpose, routine uses, and potential consequences of not providing information could reveal the investigative interests of TSA, as well as the nature and scope of an investigation, the disclosure of which could enable individuals to circumvent agency regulations or statutes.

(5) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

(b) *Transportation Workers Employment Investigations System (DHS/TSA 002).* The Transportation Workers Employment Investigations System (TWEI) (DHS/TSA 002) enables TSA to facilitate the performance of background checks on employees of transportation operators and others who are issued credentials or clearances by transportation operators, other than TSA employees. Pursuant to exemptions (k)(1) and (k)(2) of the Privacy Act, DHS/TSA 002 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures), because release of the accounting of disclosures could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency, as the individual who is the subject of a record would learn of third-agency investigate interests and thereby avoid detection or apprehension.

(2) From subsection (d) (Access to Records), because access to the records contained in this system could reveal investigate techniques and procedures in the transportation workers employment investigation process, as well as the nature and scope of the employment investigation, the disclosure of

which could enable individuals to circumvent agency regulations or statutes and obtain access to sensitive information and restricted areas in the transportation industry. The information contained in the system might include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information could reveal sensitive security information protected pursuant to 49 U.S.C. 114(s), the disclosure of which could be detrimental to the security of transportation.

(3) From subsection (e)(1) (Relevancy and Necessity of Information), because third-agency records obtained or made available to TSA during the course of an employment investigation may occasionally contain information that is not strictly relevant or necessary to a specific employment investigation. In the interests of administering an effective and comprehensive transportation worker employment investigation program, it is appropriate and necessary for TSA to retain all such information that may aid in that process.

(4) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

(c) *Personnel Background Investigation File System (DHS/TSA 004).* The Personnel Background Investigation File System (PBIFS) (DHS/TSA 004) enables TSA to maintain investigative and background material used to make suitability and eligibility determinations regarding current and former TSA employees, applicants for TSA employment, and TSA contract employees. Pursuant to exemptions (k)(1) and (k)(5) of the Privacy Act, the Personnel Background Investigation File System is exempt from 5 U.S.C. 552a(c)(3) (Accounting of Disclosures) and (d) (Access to Records). Exemptions from the particular subsections are justified because this system contains investigatory material compiled solely for determining suitability, eligibility, and qualifications for Federal civilian employment. To the extent that the disclosure of material would reveal any classified material or the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence, the applicability of exemption (k)(5) will be required to honor promises of confidentiality should the data subject request access to or amendment of the record, or access to the accounting of disclosures of the record. Exemption (k)(1) will be required to protect any classified information that may be in this system.

(d) *Internal Investigation Record System (DHS/TSA 005).* The Internal Investigation Record System (IIRS) (DHS/TSA 005) contains records of internal investigations for all modes of transportation for which TSA has security-related duties. This system covers information regarding investigations of allegations or appearances of misconduct of current or former TSA employees or contractors and provides support for any adverse action that may occur as a result of the findings of the investigation. It is being modified to cover investigations of security-related incidents and reviews of TSA programs and operations. Pursuant to exemptions (j)(2), (k)(1), and (k)(2) of the Privacy Act, DHS/TSA 005 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(3), (e)(4)(G), (H), and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could, therefore, present a serious impediment to law enforcement efforts on the part of the recipient agency, as the individual who is the subject of a record would learn of third-agency investigative interests and thereby avoid detection or apprehension, as well as to TSA investigative efforts.

(2) From subsection (d) (Access to Records) because access to the records contained in this system could reveal

investigative techniques and procedures of the investigators, as well as the nature and scope of the investigation, the disclosure of which could enable individuals to circumvent agency regulations or statutes. The information contained in the system might include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such records could reveal sensitive security information protected pursuant to 49 U.S.C. 114(s), the disclosure of which could be detrimental to the security of transportation.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because third agency records obtained or made available to TSA during the course of an investigation may occasionally contain information that is not strictly relevant or necessary to a specific investigation. In the interests of administering an effective and comprehensive investigation program, it is appropriate and necessary for TSA to retain all such information that may aid in that process.

(4) From subsection (e)(3) (Privacy Act Statement) because disclosing the authority, purpose, routine uses, and potential consequences of not providing information could reveal the targets of interests of the investigating office, as well as the nature and scope of an investigation, the disclosure of which could enable individuals to circumvent agency regulations or statutes.

(5) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

(e) *Correspondence and Matters Tracking Records (DHS/TSA 006).* The Correspondence and Matters Tracking Records (CMTR) (DHS/TSA 006) system allows TSA to manage, track, retrieve, and respond to incoming correspondence, inquiries, claims and other matters presented to TSA for disposition, and to monitor the assignment, disposition and status of such matters. This system covers information coming into TSA from individuals as well as information recorded by TSA employees in the performance of their duties. Pursuant to exemptions (k)(1) and (k)(2) of the Privacy Act, DHS/TSA 006 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures), because release of the accounting of disclosures could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency, as the individual who is the subject of a record would lean of third-agency investigative interests and thereby avoid detection or apprehension.

(2) From subsection (d) (Access to Records), because access to the records contained in this system could reveal investigative interest on the part of TSA or other agency and the nature of that interest, the disclosure of which could enable individuals to circumvent agency regulations or statutes. The information contained in the system might include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information could reveal sensitive security information protected pursuant to 49 U.S.C. 114(s), the disclosure of which could be detrimental to transportation security.

(3) From subsection (e)(1) (Relevancy and necessity of Information), because third-agency records obtained or made available to TSA during the course of an investigation may occasionally contain information that is not strictly relevant or necessary to a specific investigation. In the interests of administering an effective and comprehensive investigation program, it is appropriate and necessary for TSA to retain all such information that may aid in that process.

(4) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency rules), because this system is exempt from the access provisions of subsection (d).

(f) *Freedom of Information and Privacy Act Records (DHS/TSA 007).* The Freedom of Information and Privacy Act (FOIA/PA) Records System (DHS/TSA 007) system enables TSA to maintain records that will assist in processing access requests and administrative appeals under FOIA and access and amendments requests and appeals under the PA; participate in associated litigation; and assist TSA in carrying out any other responsibilities under FOIA/PA. Pursuant to exemptions (k)(1) and (k)(2) of the Privacy Act, Freedom of Information and Privacy Act Records are exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures), because release of the accounting of disclosures could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency, as the individual who is the subject of a record would learn of third-agency investigative interests and thereby avoid detection or apprehension.

(2) From subsection (d) (Access to Records), because access to the records contained in this system could reveal investigative interest on the part of TSA or other agency and the nature of that interest, the disclosure of which could enable individuals to circumvent agency regulations or statutes. The information contained in the system might include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information could reveal sensitive security information protected pursuant to 49 U.S.C. 114(s), the disclosure of which would be detrimental to transportation security.

(3) From subsection (e)(1) (Relevancy and necessity of Information), because third-agency records obtained or made available to TSA during the course of an investigation may occasionally contain information that is not strictly relevant or necessary to a specific investigation. In the interests of administering an effective and comprehensive investigation program, it is appropriate and necessary for TSA to retain all such information that may aid in that process.

(4) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsection (d).

(g) *General Legal Records System (DHS/TSA 009).* The General Legal Records (GLR) System (DHS/TSA 009) enables TSA to maintain records that will assist attorneys to perform their functions within the office of Chief Counsel, to include providing legal advice, responding to claims filed by employees and others, and assisting in litigation and in the settlement of claims. Pursuant to exemptions (k)(1) and (k)(2) of the Privacy Act, DHS/TSA 009 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures), because release of the accounting of disclosures could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency, as the individual who is the subject of a record would learn of third-agency investigative interests and thereby avoid detection or apprehension.

(2) From subsection (d) (Access to Records), because access to the records contained in this system could reveal investigative interest on the part of TSA or other agency and the nature of that interest, the disclosure of which would enable individuals to circumvent agency regulations or statutes. The information contained in the system might include properly classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information could reveal sensitive security information protected pursuant to 49

U.S.C. 114(s), the disclosure of which could be detrimental to transportation security.

(3) From subsection (e)(1) (Relevancy and Necessity of Information), because third-agency records obtained or made available to TSA during the course of an investigation may occasionally contain information that is not strictly relevant or necessary to a specific investigation. In the interests of administering an effective and comprehensive investigation program, it is appropriate and necessary for TSA to retain all such information that may aid in that process.

(4) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access provisions of subsections (d).

(h) *Federal Flight Deck Officer Records System (DHS/TSA 013).* The Federal Flight Deck Officer Record System (FFDORS) (DHS/TSA 013) enables TSA to maintain a system of records documenting the application, selection, training, and requalification of pilots deputized by TSA to perform the duties of a Federal Flight Deck Officer (FFDO). Pursuant to exemptions (k)(1), (k)(2), and (k)(6) of the Privacy Act, DHS/TSA 013 is exempt from 5 U.S.C. 552a(c)(3), (d), and (e)(1). Exemptions from the particular subsections are justified for the following reasons:

(1) From (c)(3) (Accounting of Certain Disclosures) and (d) (Access to Records), because access to the accounting of disclosures in this system could reveal the identity of a confidential source that provided information during the background check process. Without the ability to protect the identity of a confidential source, the agency's ability to gather pertinent information about candidates for the program may be limited. In addition, the system might contain information that is properly classified, the release of which would pose a threat to national security and/or foreign policy, or information the disclosure of which could be detrimental to the security of transportation pursuant to 49 U.S.C. 114(s). Finally, the agency must be able to protect against access to testing or examination material as release of this material could compromise the effectiveness of the testing and examination procedure itself. The examination material contained in this system is so similar in form and content to the examination material used in the selection process for TSA security screeners, or potential selection processes that TSA may utilize in the future, that release of the material would compromise the objectivity or fairness of the testing or examination process of those TSA employees.

(2) From (e)(1) (Relevancy and Necessity of Information), because information obtained or made available to TSA from other agencies and other sources during the evaluation of an individual's suitability for an FFDO position may occasionally include information that is not strictly relevant or necessary to the specific determination regarding that individual. In the interests of effective program administration, it is appropriate and necessary for TSA to collect all such information that may aid in the FFDO selection process.

(i) *Registered Traveler Operations Files (DHS/TSA 015).* The purpose of this system is to pre-screen and positively identify volunteer travelers using advanced identification technologies and conduct a security threat assessment to ensure that the volunteer does not pose a security threat. This system may expedite the pre-boarding process for the traveler and improve the allocation of TSA's security resources on individuals who may pose a security threat. Pursuant to exemptions (k)(1) and (k)(2) of the Privacy Act, DHS/TSA 015 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of heightened security concerns relating to an actual or potential criminal, civil, or regulatory violation to the existence of an investigative interest on the part of the Department of Homeland Security or another Federal law enforcement or other

recipient agency. Disclosure of the accounting would therefore present a serious impediment to transportation security law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the program suitability determination, which undermines the entire system.

(2) From subsection (d) (Access to Records) because access to some of the records contained in this system of records could permit the individual who is the subject of a record to impede the program suitability determination. Amendment of the records would interfere with ongoing security assessment investigations and program suitability determinations and impose an impossible administrative burden by requiring such investigations to be continuously reinvestigated. The information contained in the system may also include classified information, the release of which would pose a threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose sensitive security information protected pursuant to 49 U.S.C. 114(s) and 49 CFR part 1520, the disclosure of which could be detrimental to transportation security.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of screening applicants for program suitability, TSA must be able to review information from a variety of sources. What information is relevant and necessary may not always be apparent until after the evaluation is completed. In the interests of transportation security, it is appropriate to include a broad range of information that may aid in determining an applicant's suitability for the Registered Traveler program.

(4) From subsections (e)(4)(G), (H) and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access and amendment provisions of subsection (d).

(j) *Transportation Security Intelligence Service (TSIS) Operations Files.* Transportation Security Intelligence Service Operations Files (TSIS) (DHS/TSA 011) enables TSA to maintain a system of records related to intelligence gathering activities used to identify, review, analyze, investigate, and prevent violations or potential violations of transportation security laws. This system also contains records relating to determinations about individuals' qualifications, eligibility, or suitability for access to classified information. Pursuant to exemptions (j)(2), (k)(1), (k)(2), and (k)(5) of the Privacy Act, DHS/TSA 011 is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f). Exemptions from particular subsections are justified for the following reasons:

(1) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of intelligence gather operations and reveal investigative interest on the part of the Transportation Security Administration, as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to transportation security law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede operations and avoid detection and apprehension, which undermined the entire system. Disclosure of the accounting may also reveal the existence of information that is classified or sensitive security information, the release of which would be detrimental to the security of transportation.

(2) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of intelligence gathering operations and reveal investigative interest on the part of the Transportation Security Administration. Access to the records would permit the individual who is the subject of a record to impede operations and possibly avoid detection or apprehension. Amendment of the records would interfere with ongoing intelligence and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continually reinvestigated. The information contained in the system may also include properly classified information, the release of which would pose a

threat to national defense and/or foreign policy. In addition, permitting access and amendment to such information also could disclose sensitive security information, which could be detrimental to transportation security if released. This system may also include information necessary to make a determination as to an individual's qualifications, eligibility, or suitability for access to classified information, the release of which would reveal the identity of a source who received an express or implied assurance that their identity would not be revealed to the subject of the record.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of gathering and analyzing information about potential threats to transportation security, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific operation. In the interests of transportation security, it is appropriate to retain all information that may aid in identifying threats to transportation security and establishing other patterns of unlawful activity.

(4) From subsections (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules), because this system is exempt from the access and amendment provisions of subsection (d).

(k) *Secure Flight Records.* (1) Secure Flight Records (DHS/TSA 019) enables TSA to maintain a system of records related to watch list matching applied to air passengers and to non-traveling individuals authorized to enter an airport sterile area. Pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), TSA is claiming the following exemptions for certain records within the Secure Flight Records system: 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g).

(2) In addition to records under the control of TSA, the Secure Flight system of records may include records originating from systems of records of other law enforcement and intelligence agencies which may be exempt from certain provisions of the Privacy Act. However, TSA does not assert exemption to any provisions of the Privacy Act with respect to information submitted by or on behalf of individual passengers or non-travelers in the course of making a reservation or seeking access to a secured area under the Secure Flight program.

(3) To the extent the Secure Flight system contains records originating from other systems of records, TSA will rely on the exemptions claimed for those records in the originating system of records. Exemptions for certain records within the Secure Flight Records system from particular subsections of the Privacy Act are justified for the following reasons:

(i) From subsection (c)(3) (Accounting for Disclosures) because giving a record subject access to the accounting of disclosures from records concerning him or her could reveal investigative interest on the part of the recipient agency that obtained the record pursuant to a routine use. Disclosure of the accounting could therefore present a serious impediment to law enforcement efforts on the part of the recipient agency because the individual who is the subject of the record would learn of third agency investigative interests and could take steps to evade detection or apprehension. Disclosure of the accounting also could reveal the details of watch list matching measures under the Secure Flight program, as well as capabilities and vulnerabilities of the watch list matching process, the release of which could permit an individual to evade future detection and thereby impede efforts to ensure transportation security.

(ii) From subsection (c)(4) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(iii) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement counterterrorism, investigatory and intelligence records. Compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise

sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism, law enforcement, or intelligence investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(iv) From subsection (e)(1) because it is not always possible for TSA or other agencies to know in advance what information is both relevant and necessary for it to complete an identity comparison between aviation passengers or certain non-travelers and a known or suspected terrorist. In addition, because TSA and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(v) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it would put the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations, it is not feasible to rely upon information furnished by the individual concerning his own activities.

(vi) From subsection (e)(3), to the extent that this subsection is interpreted to require TSA to provide notice to an individual if TSA or another agency receives or collects information about that individual during an investigation or from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(vii) From subsections (e)(4)(G) and (H) (Agency Requirements) and (f) (Agency Rules), because this system is exempt from the access provisions of 5 U.S.C. 552a(d).

(viii) From subsection (e)(5) because many of the records in this system coming from other system of records are derived from other domestic and foreign agency record systems and therefore it is not possible for TSA to ensure their compliance with this provision, however, TSA has implemented internal quality assurance procedures to ensure that data used in the watch list matching process is as thorough, accurate, and current as possible. In addition, in the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. However, TSA has implemented internal quality assurance procedures to ensure that the data used in the watch list matching process is as thorough, accurate, and current as possible.

(ix) From subsection (e)(8) because to require individual notice of disclosure of information due to compulsory legal

process would pose an impossible administrative burden on TSA and other agencies and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(x) From subsection (f) (Agency Rules) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(xi) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

[69 FR 35537, June 25, 2004, as amended at 70 FR 33384, June 8, 2005; 71 FR 44227, Aug. 4, 2006; 72 FR 63709, Nov. 9, 2007]

PART 1510—PASSENGER CIVIL AVIATION SECURITY SERVICE FEES

Sec.

AUTHORITY: 49 U.S.C. 114, 40113, and 44940.

SOURCE: 66 FR 67701, Dec. 31, 2001, unless otherwise noted.

§ 1510.1 Applicability and purpose.

This part prescribes a uniform fee to be paid by passengers of direct air carriers and foreign air carriers in air transportation, foreign air transportation, and intrastate air transportation originating at airports in the United States to pay for the costs of providing civil aviation security services as described in 49 U.S.C. 44940.

§ 1510.3 Definitions.

The following definitions apply in this part:

Administrator means the Administrator of the Transportation Security Administration or the Administrator's designee.

Air carrier means a citizen of the United States who undertakes directly to engage in or provide air transportation.

Air transportation means intrastate, interstate or foreign air transportation.

Aircraft means a device that is used or intended to be used for flight in the air.

Airport means any landing area used regularly by aircraft for receiving or discharging passengers or cargo.

Direct air carrier and foreign air carrier means a selling carrier.

Foreign air carrier means any person other than a citizen of the United States who undertakes directly to engage in or provide air transportation.

Foreign air transportation means the carriage by aircraft of persons for compensation or hire between a place in the United States and any place outside of the United States.

Frequent flyer award means a zero-fare award of air transportation that a domestic air carrier or foreign air carrier provides to a passenger in exchange for accumulated travel mileage credits in a customer loyalty program, whether or not the term frequent flyer is used in the definition of that program.

Interstate air transportation means the carriage by aircraft of persons for compensation or hire within the United States.

Intrastate air transportation means the carriage of persons for compensation or hire wholly within the same State of the United States.

Nonrevenue passenger means a passenger receiving air transportation from an air carrier or foreign air carrier for which the air carrier or foreign air carrier does not receive remuneration.

One-way trip means any trip that is not a round trip.

Origin point means the location at which a trip on a complete air travel itinerary begins.

Passenger enplanement means a person boarding in the United States in scheduled or nonscheduled service on aircraft in intrastate, interstate, or foreign air transportation.

Principal means the aggregate amount of all passenger security services fees due to be remitted to the

Transportation Security Administration by an air carrier as required by this part.

Round trip means a trip on an air travel itinerary that terminates at the origin point.

Selling carrier means an air carrier or foreign air carrier that provides or offers to provide air transportation and has control over the operational functions performed in providing that air transportation.

[66 FR 67701, Dec. 31, 2001, as amended at 68 FR 49720, Aug. 19, 2003]

§ 1510.5 Imposition of security service fees.

(a) The security service fee will be $2.50 per passenger enplanement. The security service fee is imposed only on passengers of direct air carriers and foreign air carrier described in §1510.9(a). Passengers may not be charged for more than two enplanements per one-way trip or four enplanements per round trip.

(b) The security service fee will be imposed on all flight segments originating at an airport in the United States.

(c) The security service fee must be imposed on passengers who obtained the ticket for air transportation with a frequent flyer award, but may not be imposed on any other nonrevenue passengers.

(d) Passengers enplaning a flight segment outside of the United States are not subject to the security service fee for that enplanement.

§ 1510.7 Air transportation advertisements and solicitations.

A direct air carrier and foreign air carrier must identify the security service fee imposed by this part as ''September 11th Security Fee'' in all its advertisements and solicitations for air transportation.

§ 1510.9 Collection of security service fees.

(a) The following direct air carriers and foreign air carriers must collect security service fees from passengers enplaning:

(1) A scheduled passenger or public charter passenger operation with an aircraft having passenger seating configuration of more than 60 seats.

(2) A scheduled passenger or public charter passenger operation with an aircraft having a passenger seating configuration of less than 61 seats when passengers are enplaned from or deplaned into a sterile area.

(b) Direct air carriers and foreign air carriers must collect from each passenger, to the extent provided in §1510.5, a security service fee on air transportation sold on or after February 1, 2002. The security service fee must be based on the air travel itinerary at the time the air transportation is sold. Any changes by the passenger to the itinerary that alter the number of enplanements are subject to additional collection or refund of the security service fee by the direct air carrier or foreign air carrier as appropriate. Direct air carriers and foreign air carriers are solely liable to TSA for additional security service fees imposed because of involuntary enplanement changes to the itinerary.

(c) Whether or not the security service fee is collected as required by this part, the direct air carrier or foreign air carrier selling the air transportation is solely liable to TSA for the fee and must remit the fee as required in §1510.13.

(d) Direct air carriers and foreign air carriers may not collect security service fees not imposed by this part.

§ 1510.11 Handling of security service fees.

(a) Direct air carriers and foreign air carriers are responsible for the safekeeping of all security service fees from the time of collection to remittance.

(b) Security service fees collected by a direct air carrier or foreign air carrier are held in trust by that direct carrier for the beneficial interest of the United States in paying for the costs of providing civil aviation security services described in 49 U.S.C. 44940. The direct air carrier or foreign air carrier holds neither legal nor equitable interest in the security service fees except for the right to retain any accrued interest on the principal amounts collected pursuant to §1510.13(b).

(c) Direct air carriers and foreign air carriers must account for security service fees separately, but the fees may be commingled with the carriers' other sources of revenue.

(d) Direct air carriers and foreign air carriers must disclose in their financial statements the existence and the amount of security service fee held in trust.

§ 1510.13 Remittance of security service fees.

(a) Each direct air carrier and foreign air carrier must remit all security service fees imposed each calendar month to TSA, as directed by the Administrator, by the last calendar day of the month following the imposition.

(b) Direct air carriers and foreign air carriers may retain any interest that accrues on the principal amounts collected between the date of collection and the date the fee is remitted to TSA in accordance with paragraph (a) of this section.

(c) Direct air carriers and foreign air carriers are prohibited from retaining any portion of the principal to offset the costs of collecting, handling, or remitting the passenger security service fees.

(d) Security service fees are payable to the ''Transportation Security Administration'' in U.S. currency and drawn on a U.S. bank.

(1) Fees of $1,000 or more must be remitted by electronic funds transfer.

(2) Fees under $1,000 may be remitted by electronic funds transfer, check, money order, wire transfer, or draft.

(e) Direct air carriers and foreign air carriers are responsible for paying any bank processing charges on the security service fees collected or remitted under this part when such charges are assessed on the U.S. government.

§ 1510.15 Accounting and auditing requirements.

(a) Direct air carriers and foreign air carriers must establish and maintain an accounting system to account for the security service fees imposed, collected, refunded and remitted. The accounting records must identify the airports at which the passengers were enplaned.

(b) Each direct air carrier and foreign air carrier that collects security services fees from more than 50,000 passengers annually must provide for an audit at least annually of its security service fee activities or accounts.

(c) Audits pursuant to paragraph (b) of this section must be performed by an independent certified public accountant and may be of limited scope. The accountant must express an opinion on the fairness and reasonableness of the direct air carrier's and foreign air carrier's procedures for collecting, holding, and remitting the fees. The opinion must also address whether the quarterly reports required in §1510.17 fairly represent the net transactions in the security service fee accounts.

§ 1510.17 Reporting requirements.

(a) Each direct air carrier and foreign air carrier collecting security service fees must provide TSA with quarterly reports that provide an accounting of fees imposed, collected, refunded and remitted.

(b) Quarterly reports must state:

(1) The direct air carrier or foreign air carrier involved;

(2) The total amount of September 11th Security Fees imposed on passengers in U.S. currency for each month during the previous quarter of the calendar year;

(3) The net amount of September 11th Security Fees collected in U.S. currency by the direct air carrier or foreign air carrier for each month during the previous quarter of the calendar year;

(4) The total amount of September 11th Security Fees refunded in U.S. currency by the direct air carrier or foreign air carrier for each month during the previous quarter of the calendar year; and

(5) The total amount of September 11th Security Fees remitted in U.S. currency by the direct air carrier or foreign air carrier for each month during the previous quarter of the calendar year.

(c) The report must be filed by the last day of the calendar month following the quarter of the calendar year in which the fees were imposed.

[66 FR 67701, Dec. 31, 2001, as amended at 67 FR 14881, Mar. 28, 2002]

§ 1510.19 Federal oversight.

Direct air carriers and foreign air carriers must allow any authorized representative of the Administrator, the Secretary of Transportation, the Secretary of Homeland Security, the Inspector General of the Department of Transportation, the Inspector General of the Department of Homeland Security, or the Comptroller General of the United States to audit or review any of its books and records and provide any other information necessary to verify that the security service fees were properly collected and remitted consistent with this part.

[68 FR 49720, Aug. 19, 2003]

§ 1510.21 Enforcement.

A direct air carrier's or foreign air carrier's failure to comply with the requirements 49 U.S.C. 44940 or the provisions of this part may be considered to be an unfair and deceptive practice in violation of 49 U.S.C. 41712 and may also result in a claim due the United States by the carrier collectable pursuant to 49 CFR part 89. These remedies are in addition to any others remedies provided by law.

PART 1511—AVIATION SECURITY INFRASTRUCTURE FEE

Sec.

AUTHORITY: 49 U.S.C. 114, 40113, 44901, and 44940.

SOURCE: 67 FR 7929, Feb. 20, 2002, unless otherwise noted.

§ 1511.1 Applicability and purpose.

(a) This part prescribes the imposition of a fee on air carriers and foreign air carriers in air transportation to pay for the costs of providing U.S. civil aviation security services as described in 49 U.S.C. 44940.

(b) For purposes of this part, the fee will be described as the ''Aviation Security Infrastructure Fee.''

§ 1511.3 Definitions.

The following definitions apply for purposes of this part. For other definitions that may be applicable to this part refer to 49 U.S.C. 40102.

Administrator means the Administrator of the Transportation Security Administration or the Administrator's designee.

Air transportation means the carriage by passenger aircraft of persons or property for compensation or hire in intrastate air transportation, interstate air transportation, or foreign air transportation.

Aircraft means a device that is used or intended to be used for flight in the air.

Fiscal year means the fiscal year for the Federal government, which begins each year October 1 and ends on September 30. The fiscal year is designated by the calendar year in which it ends, *e.g.*, fiscal year 2002 is the year beginning October 1, 2001, and ending September 30, 2002.

Foreign air transportation means air transportation between a place in the United States and any place outside of the United States.

Interstate air transportation means air transportation within the United States.

Intrastate air transportation means air transportation wholly within the same State of the United States.

Passenger aircraft means an aircraft that is used to transport passengers in air transportation.

Property means mail, cargo, carry-on and checked baggage, and any other articles transported by passenger aircraft operated by an air carrier or foreign air carrier in air transportation, but excluding property transported under the ''Known Shipper Program.''

[67 FR 7929, Feb. 20, 2002, as amended at 68 FR 49720, Aug. 19, 2003]

§ 1511.5 Imposition of Aviation Security Infrastructure Fees.

(a) Effective February 18, 2002, an Aviation Security Infrastructure Fee

will be imposed on air carriers and foreign air carriers engaged in air transportation.

(b) The amount of the Aviation Security Infrastructure Fee for each fiscal year will not exceed, in the aggregate, the amounts paid in calendar year 2000 by air carriers and foreign air carriers for the screening of passengers and property transported by passenger aircraft in the United States, as determined by the Administrator.

(c) For fiscal years 2002, 2003 and 2004, the amount of the Aviation Security Infrastructure Fee imposed on each air carrier and foreign air carrier will not exceed the amount each such carrier paid for the screening of passengers and property transported by passenger aircraft in the United States during calendar year 2000, as determined by the Administrator.

(d) Each air carrier and foreign air carrier that paid for the screening of passengers and property in calendar year 2000 must fully complete the form set forth in Appendix A to this part titled, ''Calendar Year 2000 Costs Paid for Passenger and Property Screening,'' and submit the completed form to the Transportation Security Administration by May 18, 2002.

(e) In the case of a merger, acquisition, corporate restructuring, reorganization, or name change involving an air carrier or foreign air carrier that paid for the screening of passengers and property transported by passenger aircraft in the United States during calendar year 2000, the successor entity must include those screening costs in Appendix A of this part and submit those costs together with its own costs on one form in accordance with paragraph (d) of this section. Any other air carrier or foreign air carrier that paid for the screening of passengers and property transported by passenger aircraft in the United States during calendar year 2000 but is no longer providing air transportation must also complete the form set forth in Appendix A and submit the form in accordance with paragraph (d) of this section.

(f) The Administrator has determined that the information submitted pursuant to this part and 49 U.S.C. 44940(a)(2)(B) is Sensitive Security Information and is subject to the non-disclosure requirements of 49 U.S.C. 40119(b).

(g) The amount of the Aviation Security Infrastructure Fee imposed on each air carrier and foreign air carrier will be redetermined for fiscal years 2005 and beyond, and such redeterminations may be based on the carrier's respective market share or any other appropriate measure in lieu of the measure provided in paragraph (c) of this section.

§ 1511.7 Remittance of Aviation Security Infrastructure Fees.

(a) No later than May 31, 2002, each air carrier and foreign air carrier engaged in air transportation must remit to TSA.

(1) 3.273 percent of the total amount the carrier has indicated in Appendix A of this part, or an amount as otherwise determined by the Administrator, which will represent the Aviation Security Infrastructure Fee due for the period running from February 18 through February 28, 2002; and,

(2) 16.666 percent of the total amount the carrier has indicated in Appendix A of this part, or an amount as otherwise determined by the Administrator, which will represent the Aviation Security Infrastructure Fee due for period running from March 1 through April 30, 2002.

(b) Each air carrier and foreign air carrier engaged in air transportation must remit to TSA 8.333 percent of the total amount the carrier has indicated in Appendix A of this part, or an amount as otherwise determined by the Administrator, by the last calendar day of each month following May 2002 up to and including September 2004.

(c) Each air carrier and foreign air carrier engaged in air transportation must remit to TSA 8.333 percent of the total amount as determined by the Administrator pursuant to section 1511.5(g) of this part by the last calendar day of each month following September 2004.

(d) Aviation Security Infrastructure Fees must be payable to the ''Transportation Security Administration'' in U.S. currency and drawn on a U.S. bank.

(1) Aviation Security Infrastructure Fees of $1,000 or more must be remitted by electronic funds transfer.

(2) Aviation Security Infrastructure Fees under $1,000 may be remitted by electronic funds transfer, check, money order, wire transfer, or draft.

(e) Air carriers and foreign air carriers are responsible for paying any bank processing charges on Aviation Security Infrastructure Fees remitted under this part when such charges are assessed on the U.S. government.

[67 FR 7929, Feb. 20, 2002; 67 FR 8579, Feb. 25, 2002]

§ 1511.9 Accounting and auditing requirements.

(a) Each air carrier and foreign air carrier must submit an audit performed by an independent certified public accountant of the information provided pursuant to this part to the Transportation Security Administration by July 1, 2002. The cost of the audit will be borne by the carrier. The accountant must express an opinion as to the fairness and reasonableness of the air carrier's and foreign air carrier's procedures used for accounting and remitting the fees. The accountant's working papers with respect to the audit must accompany this submission.

(b) Each air carrier and foreign air carrier must maintain and retain any and all documents, records, or information related to the amount of the Aviation Security Infrastructure Fees imposed on the carrier pursuant to this part, including all information applicable to the costs submitted in Appendix A, and information that is reasonably necessary to complete an audit.

§ 1511.11 Federal oversight.

(a) Upon request, air carriers and foreign air carriers must allow any authorized representative of the Administrator, the Secretary of Transportation, the Secretary of Homeland Security, the Inspector General of the Department of Transportation, the Inspector General of the Department of Homeland Security, or the Comptroller General of the United States to audit or review any of the books and records and provide any other information necessary to verify that:

(1) The information submitted pursuant to 49 U.S.C. 44940(a)(2)(B) and this part, including that provided in Appendix A, is true and correct; or

(2) The Aviation Security Infrastructure Fees were remitted consistent with this part.

[67 FR 7929, Feb. 20, 2002, as amended at 68 FR 49720, Aug. 19, 2003]

§ 1511.13 Enforcement.

(a) In addition to any other remedies allowed by law, willful falsification by any party, directly or indirectly, of information provided by an air carrier or foreign air carrier pursuant to this part, including information submitted in Appendix A as required by section 1511.5 of this part, may be prosecuted criminally resulting in a fine and/or imprisonment under 18 U.S.C 1001.

(b) An air carrier's or foreign air carrier's failure to comply with the requirements of 49 U.S.C. 44940 or the provisions of this part may result in a claim due the United States by the carrier, which claim shall be collectable pursuant to 31 U.S.C. Chapter 37 and the Department of Transportation's implementing regulations at 49 CFR part 89.

Appendix A to Part 1511—Aviation Security Infrastructure Fee

Instructions

General guidance

When filling out this form, the responding air carrier or foreign air carrier shall include all costs incurred in calendar year 2000 by that air carrier for the screening of passengers and property. Costs are those attributed to the screening of passengers and property in the United States for both flights within the United States and flights from the United States to foreign destinations. Reported costs must be consistent with the air carrier's financial accounting information reported in accordance with generally accepted accounting principles.

Where actual costs of screening passengers and property cannot be directly identified through an air carrier's accounting system, the air carrier shall use an appropriate alternate cost assignment methodology. Documentation that explains and supports the assignment methodology used, the applicable pool and the allocation basis must be made available upon request. For costs related to capitalized property, please report the associated depreciation expense incurred during

calendar year 2000. Capitalization policy must also be made available upon request.

To the extent necessary, the reporting air carrier may aggregate those specific costs that have been incurred but cannot be stated in the detailed cost categories requested by this form. However, all of the costs identified by this form must be included in the total calculations. In addition, explanations regarding costs that have been aggregated need to be provided. Costs reported in Appendix A do not need to include costs that may have been incurred for a position higher than those of the air carrier's director of security (or equivalent). Costs incurred for higher positions, such as those of the air carrier's chief executive officer, do not need to be included.

When including cost information on acquired and/or merged air carriers, the successor air carrier must specify the names of all of such entities whose calendar year 2000 passenger and property screening costs are included in that air carrier's submission as Appendix A.

The costs listed below are to be in US dollars, rounded to the nearest dollar. Place a zero in the appropriate box to indicate cost categories in which the air carrier did not incur costs for passenger and property screening in calendar year 2000.

Supporting Notes

Examples of cost types that appear in the supporting notes below are for illustrative purposes only and are not intended to set forth all relevant costs that must be reported by air carriers and foreign air carriers. In submitting information to TSA, air carriers and foreign air carriers must submit all of their relevant costs, regardless of whether those costs have been specifically illustrated in the notes.

Submission of Data

This form will be available electronically from the Department of Transportation's website at *www.dot.gov*. Air carriers are asked to return the completed form by certified mail to: Chief Financial Officer, Transportation Security Administration, Department of Transportation, 400 Seventh Street SW, Washington, DC 20590. Please also submit the same information in Microsoft Word either on a computer disk or by e-mail to *TSA-Fees@ost.dot.gov*.

Confidentiality of Data

Consistent with 49 CFR §1511.5(f), information submitted in Appendix A is deemed to be Sensitive Security Information and will be so protected from public disclosure under 49 U.S.C. 40119(b). In addition, confidential business information and economic information provided in Appendix A will be protected from public disclosure, as appropriate, under 5 U.S.C. §552 (the Freedom of Information Act), 14 CFR §302.12, and 18 U.S.C. §1905. Requests for confidentiality must be filed with the Office of the General Counsel, Department of Transportation (C–10), 400 Seventh Street, SW, Room 10102, Washington, DC 20590.

Calendar Year 2000 Costs for Passenger and Property Screening

Air Carrier name(s): _____ Date Form Completed: _____

		Cost Categories	Costs Incurred Directly by Air Carriers[a]	Costs Incurred Through Security Firm Contracts[b]	Costs Incurred Through Other Means[c]	Total Costs Incurred
A) Screening Personnel and Supervisors:	1	Checkpoint Screening Personnel				
	2	Exit Lane Monitors				
	3	Cargo Screeners				
	4	Checked Baggage Screeners				
	5	Baggage Runners				
	6	Supervisory Personnel				
	7	Non-Labor Costs				
	8	Background Checks				
	9	Training and Testing				
	10	Training Records				
	11	Evaluations				
	12	Drug and Alcohol Testing and Treatment				

25

		Cost Categories	Costs Incurred Directly by Air Carriers	Costs Incurred Through Security Firm Contracts[b]	Costs Incurred Through Other Means[c]	Total Costs Incurred
	13	Uniforms				
	14	Canines				
	15	Cost of Obtaining Security Clearances				
		Total for Section A				
B) Equipment and Procedures:	16	Screening Equipment Installation				
	17	Operating, Operational Maintenance and Testing of Installed Screening Equipment				
	18	Maintenance of Sterile Areas				
	19	Checkpoint Signs and Related Equipment				
	20	Exceptional Screening for Persons and Property				
	21	Security Company Contracts				
		Total for Section B				
C) Property and Plant:	22	Real Estate				
	23	Utilities				
		Total for Section C				

		Cost Categories	Costs Incurred Directly by Air Carriers	Costs Incurred Through Security Firm Contracts[b]	Costs Incurred Through Other Means[c]	Total Costs Incurred
D) Program Management and Contract Oversight:	24	Ground Security Coordinators				
	25	Security Program Management				
	26	Security Contract Administration and Oversight				
	27	Screener/Supervisor Background Check Audits				
	28	Legal Support				
	29	Accounting Support				
	30	Other Administrative Support				
	31	Insurance				
	32	Law Enforcement Costs				
	33	Recruitment Expenses				
		Total for Section D				
E) Security Consortium Costs:	34	Management Fees for Oversight of Consortium Contracts				
		Total for Section E				

27

		Cost Categories	Costs Incurred Directly by Air Carriers	Costs Incurred Through Security Firm Contracts[b]	Costs Incurred Through Other Means[c]	Total Costs Incurred
F) Other:	35	Other				
		Total for Section F				
Total for all Sections:						

Supporting Notes

a. These are costs that the air carrier incurred directly. Includes costs incurred for air carrier personnel salaries and benefits, equipment owned, leased or rented directly by that air carrier and any other costs directly incurred.

b. These are costs that the air carrier incurred through contracts with security firms. Includes personnel, equipment and other costs incurred through contracts with third party security companies.

c. These are costs that the air carrier incurred through other means. Includes costs incurred through air carrier security consortiums.

1. Salary, benefits, overtime, retirement and other costs of checkpoint screening personnel.

2. Salary, benefits, overtime, retirement and other costs of exit lane monitors.

3. Salary, benefits, overtime, retirement and other costs of cargo screeners.

4. Salary, benefits, overtime, retirement and other costs of checked baggage screeners.

5. Salary, benefits, overtime, retirement and other costs of all baggage runners who move property such as baggage to and from screening areas.

6. Salary, benefits, overtime, retirement and other costs of all supervisory personnel, including Checkpoint Screening Supervisors.

7. All associated expensed non-labor costs including computers, communications equipment, time management systems, supplies, parking, identification badging, furniture, fixtures, and travel.

8. All costs of performing required background investigations on all screening personnel and supervisors. Screening personnel and supervisors includes checkpoint screening personnel, exit lane monitors, cargo screeners, checked baggage screeners, baggage runners, and their supervisors.

9. All costs incurred for the training and testing of all screening personnel and supervisors, including initial, recurrent and remedial training. Includes any computer-based training and the development of training programs for the screening of persons and property as well as any travel, room and board, and all other such expenses related to training.

10. The costs of implementing and maintaining training records for all screening personnel and supervisors.

11. The costs of completing evaluations for all screening personnel and supervisors.

12. All costs for drug and alcohol testing as well as any associated counseling and/or treatment for all screening personnel and supervisors.

13. All costs of renting, purchasing, maintaining, and/or cleaning of uniforms and any related equipment such as flashlights and batons for all screening personnel and supervisors.

14. All costs incurred by air carriers for the use of canines and their handlers used for the screening of persons and property.

15. All costs associated with obtaining security clearances for personnel relating to the screening of persons and property.

16. All costs associated with the purchase, installation, and testing of all screening equipment. In instances where the equipment is capitalized, provide the depreciation expense in lieu of costs associated with purchase, installation, and final acceptance testing. This includes such equipment as Metal Detection Devices, Hand Wands, X-ray screening machines, Explosives Trace Detection Devices, Explosives Detection Systems, or any other such similar technologies. Includes any costs incurred or depreciation costs recognized in calendar year 2000 for the modification and/or construction of any facility needed to accommodate screening, including architecture and engineering. Also includes the costs of any refurbishment and/or modernization of the equipment.

17. Costs of operating, maintaining, and calibrating installed screening equipment. This includes such equipment as Metal Detection Devices, Hand Wands, X-ray screening machines, Explosives Trace Detection Devices, Explosives Detection Systems, or any other such similar technologies. Includes such costs as test objects and X-ray radiation surveys, electricity costs and maintenance contract costs incurred for the operations of such equipment.

18. Costs of maintaining integrity of sterile areas. Includes costs of opening sterile areas, emergency evacuations of sterile areas, and re-screenings not included elsewhere.

19. The cost of purchase or rent, installation, testing, and maintenance of checkpoint signs, barriers, lane markers, and exit lane doors.

20. Any additional costs for special screening such as for disabled passengers, VIP passengers, classified and/or high value items.

21. All security company contract costs for the screening of persons and property that cannot be detailed into any other cost category.

22. All direct costs for the real estate utilized for the screening of persons and property. Includes space at airports for the performance of these functions, as well as such space used for break rooms, private screening rooms, storages space, training rooms, and office space. Also includes appropriate space for the oversight of the screening functions outside of airports such as in headquarters or regional offices.

23. All costs for utilities used for screening. Includes electricity, heating/ventilation/cooling, and telecommunications costs not elsewhere specified.

24. All costs incurred for the Ground Security Coordinator's oversight of the screening functions. Includes personnel salaries, benefits, retirement, training, and non-labor costs.

25. All air carrier head office, regional, or airport specific costs associated with the administration and oversight of screening not elsewhere specified. Includes personnel salaries, benefits, retirement, training, and non-labor costs.

26. All costs associated with the administration and oversight of screening contracts. Includes personnel, benefits, retirement, training, and non-labor costs.

27. All costs not elsewhere specified for background audit checks for all screeners and supervisors.

28. All legal support costs incurred during calendar year 2000 relating to aviation security screening. Includes legal assistance for

the implementation and execution of security screening contracts.

29. All costs for accounting and financial services incurred for the support of the screening functions.

30. Includes all labor and non-labor costs for such items as human resource administration, clerical assistance, information technology, and other support functions related to screening.

31. All insurance costs relating to screening. Includes worker's compensation and general liability insurance.

32. All costs incurred by the air carriers for law enforcement personnel costs that were reimbursed by the air carriers for services performed in connection with the screening of persons and property.

33. All costs associated with the recruitment of screening personnel and supervisors. Includes signing bonuses, travel, and other recruitment expenses.

34. Any costs incurred for fees charged by other organizations for the management of contracts for the screening of persons and property.

35. Any costs incurred not elsewhere specified during calendar year 2000 for the screening of passengers and property. These costs should be itemized on a separate sheet. Includes any fines or monetary penalties incurred for screening as well as any profit/bonuses paid to contractors for screening services not included elsewhere on the form.

Certification:

I certify that the information contained in this form (Appendix A-Part 1511) is true and accurate under penalty of law. Willful falsification of any information contained in this form under Part 1511 in Title 49, Chapter XII may be prosecuted criminally and result in a fine and/or imprisonment. (18 U.S.C. 1001)

_____ _____

Certifying Officer (signature) Date

_____ _____

Print Name and Title (CEO, CFO or COO) Telephone Number

Contact Information:

Listed below are the contact name, title, address and telephone number of the person responsible for the payment of the Aviation Security Infrastructure Fees to the Transportation Security Administration:

Name: _____

Title: _____

Address: _____

_____

_____

Telephone: _____

Person Who Prepared Document:

Listed below are the contact name, title, address and telephone number of the person who prepared this document:

Name: _____

Title: _____

Address: _____

_____

_____

Telephone: _____

PART 1515—APPEAL AND WAIVER PROCEDURES FOR SECURITY THREAT ASSESSMENTS FOR INDIVIDUALS

Sec.

AUTHORITY: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

SOURCE: 72 FR 3588, Jan. 25, 2007, unless otherwise noted.

§ 1515.1 Scope.

(a) *Appeal.* This part applies to applicants who are appealing an Initial Determination of Threat Assessment or an Initial Determination of Threat Assessment and Immediate Revocation in a security threat assessment as described in:

(1) 49 CFR part 1572 for a hazardous materials endorsement (HME) or a Transportation Worker Identification Credential (TWIC); or

(2) 49 CFR part 1540, subpart C, for air cargo workers.

(b) *Waivers.* This part applies to applicants for an HME or TWIC who undergo a security threat assessment described in 49 CFR part 1572 and are eligible to request a waiver of certain standards.

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, §1515.1 was amended by revising paragraph (a), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1515.1 Scope.

(a) *Appeal.* This part applies to applicants who are appealing an Initial Determination of Threat Assessment or an Initial Determination of Threat Assessment and Immediate Revocation in a security threat assessment (STA) as described in each of the following:

(1) 49 CFR part 1572 for a hazardous materials endorsement (HME) or a Transportation Worker Identification Credential (TWIC).

(2) 49 CFR part 1540, Subpart C, which includes individuals engaged in air cargo operations who work for certain aircraft operators, foreign air carriers, IACs, certified cargo screening facilities, or validation firms.

* * * * *

§ 1515.3 Terms used in this part.

The terms used in 49 CFR parts 1500, 1540, 1570, and 1572 also apply in this part. In addition, the following terms are used in this part:

Administrative law judge means an administrative law judge appointed pursuant to the provisions of 5 U.S.C. 3105.

Applicant means an individual who has applied for one of the security threat assessments identified in 49 CFR 1515.1. This includes an individual who previously applied for and was found to meet the standards for the security threat assessment but TSA later determined that the individual poses a security threat.

Date of service means—

(1) In the case of personal service, the date of personal delivery to the residential address listed on the application;

(2) In the case of mailing with a certificate of service, the date shown on the certificate of service;

(3) In the case of mailing and there is no certificate of service, 10 days from the date mailed to the address designated on the application as the mailing address;

(4) In the case of mailing with no certificate of service or postmark, the date mailed to the address designated on the application as the mailing address shown by other evidence; or

(5) The date on which an electronic transmission occurs.

Day means calendar day.

Final Agency Order means an order issued by the TSA Final Decision Maker.

Decision denying a review of a waiver means a document issued by an administrative law judge denying a waiver requested under 49 CFR 1515.7.

Mail includes U.S. mail, or use of an express courier service.

Party means the applicant or the agency attorney.

Personal delivery includes hand-delivery or use of a contract or express messenger service, but does not include the use of Government interoffice mail service.

Properly addressed means a document that shows an address contained in agency records, a residential, business, or other address submitted by a person on any document provided under this subpart, or any other address shown by other reasonable and available means.

Substantial Evidence means such relevant evidence as a reasonable person might accept as adequate to support a conclusion.

Security threat assessment means the threat assessment for which the applicant has applied, as described in 49 CFR 1515.1.

TSA Final Decision Maker means the Administrator, acting in the capacity of the decision maker on appeal, or any person to whom the Administrator has delegated the Administrator's decision-making authority. As used in this subpart, the *TSA Final Decision Maker* is the official authorized to issue a final decision and order of the Administrator.

§ 1515.5 Appeal of Initial Determination of Threat Assessment based on criminal conviction, immigration status, or mental capacity.

(a) *Scope.* This section applies to applicants appealing from an Initial Determination of Threat Assessment that was based on one or more of the following:

(1) TSA has determined that an applicant for an HME or a TWIC has a disqualifying criminal offense described in 49 CFR 1572.103.

(2) TSA has determined that an applicant for an HME or a TWIC does not meet the immigration status requirements as described in 49 CFR 1572.105.

(3) TSA has determined that an applicant for an HME or a TWIC is lacking mental capacity as described in 49 CFR 1572.109.

(b) *Grounds for appeal.* An applicant may appeal an Initial Determination of Threat Assessment if the applicant is asserting that he or she meets the standards for the security threat assessment for which he or she is applying.

(1) *Initiating an appeal.* An applicant initiates an appeal by submitting a written reply to TSA, a written request for materials from TSA, or by requesting an extension of time in accordance with § 1515.5(f). If the applicant does not initiate an appeal within 60 days of receipt, the Initial Determination of Threat Assessment becomes a Final Determination of Threat Assessment.

(i) In the case of an HME, TSA also serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a mariner applying for TWIC, TSA also serves a Final Determination of Threat Assessment on the Coast Guard.

(iii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the appropriate Federal Maritime Security Coordinator (FMSC).

(2) *Request for materials.* Within 60 days of the date of service of the Initial Determination of Threat Assessment, the applicant may serve upon TSA a written request for copies of the materials upon which the Initial Determination was based.

(3) *TSA response.* (i) Within 60 days of receiving the applicant's request for materials, TSA serves the applicant with copies of the releasable materials upon the applicant on which the Initial Determination was based. TSA will not include any classified information or other protected information described in paragraph (f) of this section.

(ii) Within 60 days of receiving the applicant's request for materials or written reply, TSA may request additional information or documents from the applicant that TSA believes are necessary to make a Final Determination.

(4) *Correction of records.* If the Initial Determination of Threat Assessment was based on a record that the applicant believes is erroneous, the applicant may correct the record, as follows:

(i) The applicant contacts the jurisdiction or entity responsible for the information and attempts to correct or complete information contained in his or her record.

(ii) The applicant provides TSA with the revised record, or a certified true copy of the information from the appropriate entity, before TSA determines that the applicant meets the standards for the security threat assessment.

(5) *Reply.* (i) The applicant may serve upon TSA a written reply to the Initial Determination of Threat Assessment within 60 days of service of the Initial Determination, or 60 days after the date of service of TSA's response to the applicant's request for materials under paragraph (b)(1) of this section, if the applicant served such request. The reply must include the rationale and information on which the applicant disputes TSA's Initial Determination.

(ii) In an applicant's reply, TSA will consider only material that is relevant to whether the applicant meets the standards applicable for the security threat assessment for which the applicant is applying.

(6) *Final determination.* Within 60 days after TSA receives the applicant's reply, TSA serves a Final Determination of Threat Assessment or a Withdrawal of the Initial Determination as provided in paragraphs (c) or (d) of this section.

(c) *Final Determination of Threat Assessment.* (1) If the Assistant Administrator concludes that an HME or TWIC applicant does not meet the standards described in 49 CFR 1572.103, 1572.105, or 1572.109, TSA serves a Final Determination of Threat Assessment upon the applicant. In addition—

(i) In the case of an HME, TSA serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the Coast Guard.

(2) The Final Determination includes a statement that the Assistant Administrator has reviewed the Initial Determination, the applicant's reply and any accompanying information, and any other materials or information available to him or her, and has determined that the applicant poses a security threat warranting denial of the security threat assessment for which the applicant has applied.

(d) *Withdrawal of Initial Determination.* If the Assistant Administrator or Assistant Secretary concludes that the applicant does not pose a security threat, TSA serves a Withdrawal of the Initial Determination upon the applicant, and the applicant's employer where applicable.

(e) *Nondisclosure of certain information.* In connection with the procedures under this section, TSA does not disclose classified information to the applicant, as defined in E.O. 12968 sec. 1.1(d), and reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

(f) *Extension of time.* TSA may grant an applicant an extension of time of the limits for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended; or an applicant may request an extension after the expiration of a due date by sending a written request describing why the failure to file within the time limits was excusable. TSA may grant itself an extension of time for good cause.

(g) *Judicial review.* For purposes of judicial review, the Final Determination of Threat Assessment constitutes a final TSA order of the determination that the applicant does not meet the standards for a security threat assessment, in accordance with 49 U.S.C. 46110. The Final Determination is not a final TSA order to grant or deny a waiver, the procedures for which are in 49 CFR 1515.7 and 1515.11.

(h) *Appeal of immediate revocation.* If TSA directs an immediate revocation, the applicant may appeal this determination by following the appeal procedures described in paragraph (b) of this section. This applies—

(1) If TSA directs a State to revoke an HME pursuant to 49 CFR 1572.13(a).

(2) If TSA invalidates a TWIC by issuing an Initial Determination of Threat Assessment and Immediate Revocation pursuant to 49 CFR 1572.21(d)(3).

[72 FR 3588, Jan. 25, 2007; 72 FR 14049, Mar. 26, 2007]

§ 1515.7 Procedures for waiver of criminal offenses, immigration status, or mental capacity standards.

(a) *Scope.* This section applies to the following applicants:

(i) An applicant for an HME or TWIC who has a disqualifying criminal offense described in 49 CFR 1572.103(a)(5) through (a)(12) or 1572.103(b) and who requests a waiver.

(ii) An applicant for an HME or TWIC who is an alien under temporary protected status as described in 49 CFR 1572.105 and who requests a waiver.

(iii) An applicant applying for an HME or TWIC who lacks mental capacity as described in 49 CFR 1572.109 and who requests a waiver.

(b) *Grounds for waiver.* TSA may issue a waiver of the standards described in paragraph (a) and grant an HME or TWIC if TSA determines that an applicant does not pose a security threat based on a review of information described in paragraph (c) of this section.

(c) *Initiating waiver.* (1) An applicant initiates a waiver as follows:

(i) Providing to TSA the information required in 49 CFR 1572.9 for an HME or 49 CFR 1572.17 for a TWIC.

(ii) Paying the fees required in 49 CFR 1572.405 for an HME or in 49 CFR 1572.501 for a TWIC.

(iii) Sending a written request to TSA for a waiver at any time, but not

later than 60 days after the date of service of the Final Determination of Threat Assessment. The applicant may request a waiver during the application process, or may first pursue some or all of the appeal procedures in 49 CFR 1515.5 to assert that he or she does not have a disqualifying condition.

(2) In determining whether to grant a waiver, TSA will consider the following factors, as applicable to the disqualifying condition:

(i) The circumstances of the disqualifying act or offense.

(ii) Restitution made by the applicant.

(iii) Any Federal or State mitigation remedies.

(iv) Court records or official medical release documents indicating that the applicant no longer lacks mental capacity.

(v) Other factors that indicate the applicant does not pose a security threat warranting denial of the HME or TWIC.

(d) *Grant or denial of waivers.* (1) The Assistant Administrator will send a written decision granting or denying the waiver to the applicant within 60 days of service of the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(2) In the case of an HME, if the Assistant Administrator grants the waiver, the Assistant Administrator will send a Determination of No Security Threat to the licensing State within 60 days of service of the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(3) In the case of a mariner applying for a TWIC, if the Assistant Administrator grants the waiver, the Assistant Administrator will send a Determination of No Security Threat to the Coast Guard within 60 days of service of the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(4) If the Assistant Administrator denies the waiver the applicant may seek review in accordance with 49 CFR 1515.11. A denial of a waiver under this section does not constitute a final order of TSA as provided in 49 U.S.C. 46110.

(e) *Extension of time.* TSA may grant an applicant an extension of the time limits for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended; or an applicant may request an extension after the expiration of a due date by sending a written request describing why the failure to file within the time limits was excusable. TSA may grant itself an extension of time for good cause.

§ 1515.9 Appeal of security threat assessment based on other analyses.

(a) *Scope.* This section applies to an applicant appealing an Initial Determination of Threat Assessment as follows:

(1) TSA has determined that the applicant for an HME or TWIC poses a security threat as provided in 49 CFR 1572.107.

(2) TSA had determined that an air cargo worker poses a security threat as provided in 49 CFR 1540.205.

(b) *Grounds for appeal.* An applicant may appeal an Initial Determination of Threat Assessment if the applicant is asserting that he or she does not pose a security threat. The appeal will be conducted in accordance with the procedures set forth in 49 CFR 1515.5(b), (e), and (f) and this section.

(c) *Final Determination of Threat Assessment.* (1) If the Assistant Administrator concludes that the applicant poses a security threat, following an appeal, TSA serves a Final Determination of Threat Assessment upon the applicant. In addition—

(i) In the case of an HME, TSA serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the Coast Guard.

(iii) In the case of an air cargo worker, TSA serves a Final Determination of Threat Assessment on the operator.

(2) The Final Determination includes a statement that the Assistant Administrator has reviewed the Initial Determination, the applicant's reply and any accompanying information, and any other materials or information available to him or her, and has determined that the applicant poses a security

threat warranting denial of the security threat assessment for which the applicant has applied.

(d) *Withdrawal of Initial Determination.* If the Assistant Administrator concludes that the applicant does not pose a security threat, TSA serves a Withdrawal of the Initial Determination upon the applicant, and the applicant's employer where applicable.

(e) *Further review.* If the Assistant Administrator denies the appeal, the applicant may seek review in accordance with § 1515.11 of this part. A Final Determination issued under this section does not constitute a final order of TSA as provided in 49 U.S.C. 46110.

(f) *Appeal of immediate revocation.* If TSA directs an immediate revocation, the applicant may appeal this determination by following the appeal procedures described in paragraph (b) of this section. This applies—

(1) If TSA directs a State to revoke an HME pursuant to 49 CFR 1572.13(a).

(2) If TSA invalidates a TWIC by issuing an Initial Determination of Threat Assessment and Immediate Revocation pursuant to 49 CFR 1572.21(d)(3).

(3) If TSA withdraws a Determination of No Threat issued for an air cargo worker.

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, § 1515.9 was amended by adding paragraphs (a)(3), (c)(1)(iv) and (v) and revising (f)(3), effective November 16, 2009. For the convenience of the user, the added and revised text is set forth as follows:

§ 1515.9 Appeal of security threat assessment based on other analyses.

(a) * * *

(3) TSA had determined that an individual engaged in air cargo operations who works for certain aircraft operators, foreign air carriers, indirect air carriers (IACs), certified cargo screening facilities, or validation firms poses a security threat as provided in 49 CFR 1549.109.

* * * * *

(c) * * *

(1) * * *

(iv) In the case of a certified cargo screening facilities worker, TSA serves a Final Determination of Threat Assessment on the operator.

(v) In the case of a validator of certified cargo screening facilities, TSA serves a Final Determination of Threat Assessment on the operator.

* * * * *

(f) * * *

(3) If TSA withdraws a Determination of No Security Threat for an individual engaged in air cargo operations who works for certain aircraft operators, foreign air carriers, IACs, certified cargo screening facilities, or validation firms.

§ 1515.11 Review by administrative law judge and TSA Final Decision Maker.

(a) *Scope.* This section applies to the following applicants:

(1) An applicant who seeks review of a decision by TSA denying a request for a waiver under 49 CFR 1515.7.

(2) An applicant for an HME or a TWIC who has been issued a Final Determination of Threat Assessment on the grounds that he or she poses a security threat after an appeal as described in 49 CFR 1515.9.

(3) An air cargo worker who has been issued a Final Determination of Threat Assessment after an appeal as described in 49 CFR 1515.9.

(b) *Request for review.* No later than 30 calendar days from the date of service of the decision by TSA denying a waiver or of the Final Determination of Threat Assessment, the applicant may request a review. The review will be conducted by an administrative law judge who possesses the appropriate security clearance necessary to review classified or otherwise protected information and evidence. If the applicant fails to seek review within 30 calendar days, the Final Determination of Threat Assessment will be final with respect to the parties.

(1) The request for review must clearly state the issue(s) to be considered by the administrative law judge (ALJ), and include the following documents in support of the request:

(i) In the case of a review of a denial of waiver, a copy of the applicant's request for a waiver under 49 CFR 1515.7, including all materials provided by the applicant to TSA in support of the waiver request; and a copy of the decision issued by TSA denying the waiver request. The request for review may not include evidence or information that was not presented to TSA in the

request for a waiver under 49 CFR 1515.7. The ALJ may consider only evidence or information that was presented to TSA in the waiver request. If the applicant has new evidence or information, the applicant must file a new request for a waiver under §1515.7 and the pending request for review of a denial of a waiver will be dismissed.

(ii) In the case of a review of a Final Determination of Threat Assessment, a copy of the Initial Notification of Threat Assessment and Final Notification of Threat Assessment; and a copy of the applicant's appeal under 49 CFR 1515.9, including all materials provided by the applicant to TSA in support of the appeal. The request for review may not include evidence or information that was not presented to TSA in the appeal under §1515.9. The ALJ may consider only evidence or information that was presented to TSA in the appeal. If the applicant has new evidence or information, the applicant must file a new appeal under §1515.9 and the pending request for review of the Final Determination will be dismissed.

(2) The applicant may include in the request for review a request for an in-person hearing before the ALJ.

(3) The applicant must file the request for review with the ALJ Docketing Center, U.S. Coast Guard, 40 S. Gay Street, Room 412, Baltimore, Maryland 21202–4022, ATTN: Hearing Docket Clerk.

(c) *Extension of Time.* The ALJ may grant an extension of the time limits described in this section for good cause shown. A request for an extension of time must be in writing and be received by the ALJ within a reasonable time before the due date to be extended; or an applicant may request an extension after the expiration of a due date by sending a written request describing why the failure to file within the time limits was excusable. This paragraph does not apply to time limits set by the administrative law judge during the hearing.

(d) *Duties of the Administrative Law Judge.* The ALJ may:

(1) Receive information and evidence presented to TSA in the request for a waiver under 49 CFR 1515.7 or an appeal under 49 CFR 1515.9.

(2) Consider the following criteria to determine whether a request for an in-person hearing is warranted:

(i) The credibility of evidence or information submitted in the applicant's request for a waiver; and

(ii) Whether TSA's waiver denial was made in accordance with the governing regulations codified at 49 CFR part 1515 and 49 CFR part 1572.

(3) Give notice of and hold conferences and hearings;

(4) Administer oaths and affirmations;

(5) Examine witnesses;

(6) Regulate the course of the hearing including granting extensions of time limits; and

(7) Dispose of procedural motions and requests, and issue a decision.

(e) *Hearing.* If the ALJ grants a request for a hearing, except for good cause shown, it will begin within 60 calendar days of the date of receipt of the request for hearing. The hearing is a limited discovery proceeding and is conducted as follows:

(1) If applicable and upon request, TSA will provide to the applicant requesting a review an unclassified summary of classified evidence upon which the denial of the waiver or Final Determination was based.

(i) TSA will not disclose to the applicant, or the applicant's counsel, classified information, as defined in E.O. 12968 section 1.1(d).

(ii) TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure by law or regulation.

(2) The applicant may present the case by oral testimony, documentary, or demonstrative evidence, submit rebuttal evidence, and conduct cross-examination, as permitted by the ALJ. Oral testimony is limited to the evidence or information that was presented to TSA in the request for a waiver or during the appeal. The Federal Rules of Evidence may serve as guidance, but are not binding.

(3) The ALJ will review any classified information on an ex parte, in camera basis, and may consider such information in rendering a decision if the information appears to be material and relevant.

(4) The standard of proof is substantial evidence on the record.

(5) The parties may submit proposed findings of fact and conclusions of law.

(6) If the applicant fails to appear, the ALJ may issue a default judgment.

(7) A verbatim transcript will be made of the hearing and will be provided upon request at the expense of the requesting party. In cases in which classified or otherwise protected evidence is received, the transcript may require redaction of the classified or otherwise protected information.

(8) The hearing will be held at TSA's Headquarters building or, on request of a party, at an alternate location selected by the administrative law judge for good cause shown.

(f) *Decision of the Administrative Law Judge.* (1) The record is closed once the certified transcript and all documents and materials have been submitted for the record.

(2) The ALJ issues an unclassified written decision to the applicant no later than 30 calendar days from the close of the record and serves the decision on the parties. The ALJ may issue a classified decision to TSA.

(3) The ALJ's decision may be appealed by either party to the TSA Final Decision Maker in accordance with paragraph (g).

(i) In the case of review of a waiver denial, unless appealed to the TSA Final Decision Maker, if the ALJ upholds the denial of the applicant's request for waiver, TSA will issue a Final Order Denying a Waiver to the applicant.

(ii) In the case of review of a waiver denial, unless appealed to the TSA Final Decision Maker, if the ALJ reverses the denial of the applicant's request for waiver, TSA will issue a Final Order granting a waiver to the applicant; and

(A) In the case of an HME, send a Determination of No Security Threat to the licensing State.

(B) In the case applicant for a TWIC, send a Determination of No Security Threat to the Coast Guard.

(C) In the case of an air cargo worker, send a Determination of No Security Threat to the operator.

(iii) In the case of review of an appeal under 49 CFR 1515.9, unless appealed to the TSA Final Decision Maker, if the ALJ determines that the applicant poses a security threat, TSA will issue a Final Order of Threat Assessment to the applicant.

(iv) In the case of review of an appeal under 49 CFR 1515.9, unless appealed to the TSA Final Decision Maker, if the ALJ determines that the applicant does not pose a security threat, TSA will issue a Withdrawal of the Final Determination to the applicant, and to the applicant's employer where applicable.

(g) *Review by the TSA Final Decision Maker.* (1) Either party may request that the TSA Final Decision Maker review the ALJ's decision by serving the request no later than 30 calendar days after the date of service of the decision of the ALJ.

(i) The request must be in writing, served on the other party, and may only address whether the decision is supported by substantial evidence on the record.

(ii) No later than 30 calendar days after receipt of the request, the other party may file a response.

(2) The ALJ will provide the TSA Final Decision Maker with a certified transcript of the hearing and all unclassified documents and material submitted for the record. TSA will provide any classified materials previously submitted.

(3) No later than 60 calendar days after receipt of the request, or if the other party files a response, 30 calendar days after receipt of the response, or such longer period as may be required, the TSA Final Decision Maker issues an unclassified decision and serves the decision on the parties. The TSA Final Decision Maker may issue a classified opinion to TSA, if applicable. The decision of the TSA Final Decision Maker is a final agency order.

(i) In the case of review of a waiver denial, if the TSA Final Decision Maker upholds the denial of the applicant's request for waiver, TSA issues a Final Order Denying a Waiver to the applicant.

(ii) In the case of review of a waiver denial, if the TSA Final Decision Maker reverses the denial of the applicant's request for waiver, TSA will grant the waiver; and

(A) In the case of an HME, send a Determination of No Security Threat to the applicant and to the licensing State.

(B) In the case of a TWIC, send a Determination of No Security Threat to the applicant and to the Coast Guard.

(C) In the case of an air cargo worker, send a Determination of No Security Threat to the applicant and the operator.

(iii) In the case of review of an appeal under 49 CFR 1515.9, if the TSA Final Decision Maker determines that the applicant poses a security threat, TSA will issue a Final Order of Threat Assessment to the applicant.

(iv) In the case of review of an appeal under 49 CFR 1515.9, if the TSA Final Decision Maker determines that the applicant does not pose a security threat, TSA will issue a Withdrawal of the Final Determination to the applicant, and to the applicant's employer where applicable.

(h) *Judicial Review of a Final Order Denying a Waiver.* A person may seek judicial review of a final order of the TSA Final Decision Maker as provided in 49 U.S.C. 46110.

[72 FR 3588, Jan. 25, 2007; 72 FR 5633, Feb. 7, 2007]

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, §1511.11 was amended by revising paragraph (a)(3), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1515.11 Review by administrative law judge and TSA Final Decision Maker.

(a) * * *

(3) An individual engaged in air cargo operations who works for certain aircraft operators, foreign air carriers, IACs, certified cargo screening facilities, or validation firms who has been issued a Final Determination of Threat Assessment after an appeal as described in 49 CFR 1515.9.

* * * * *

SUBCHAPTER B—SECURITY RULES FOR ALL MODES OF TRANSPORTATION

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.

AUTHORITY: 46 U.S.C. 70102–70106, 70117; 49 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

SOURCE: 69 FR 28082, May 18, 2004, unless otherwise noted.

§ 1520.1 Scope.

(a) *Applicability*. This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information, as defined in § 1520.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation*. The authority of TSA and the Coast Guard under this part may be further delegated within TSA and the Coast Guard, respectively.

§ 1520.3 Terms used in this part.

In addition to the terms in § 1500.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in § 1520.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in § 1520.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Rail facility means ''rail facility'' as defined in 49 CFR 1580.3.

Rail hazardous materials receiver means ''rail hazardous materials receiver'' as defined in 49 CFR 1580.3.

Rail hazardous materials shipper means ''rail hazardous materials shipper'' as defined in 49 CFR 1580.3.

Rail secure area means ''rail secure area'' as defined in 49 CFR 1580.3.

Rail transit facility means ''rail transit facility'' as defined in 49 CFR 1580.3.

Rail transit system or *Rail Fixed Guideway System* means ''rail transit system'' or ''Rail Fixed Guideway System'' as defined in 49 CFR 1580.3.

Railroad means ''railroad'' as defined in 49 U.S.C. 20102(1).

Railroad carrier means ''railroad carrier'' as defined in 49 U.S.C. 20102(2).

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term *record* also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments, developed for the security of the following, including any comments, instructions, or implementing guidance:

(1) An airport, aircraft, or aviation cargo operation;

(2) A fixed base operator;

(3) A maritime facility, vessel, or port area; or

(4) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in §1520.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, or vessel; aircraft; railroad; railroad carrier, rail facility; train; rail hazardous materials shipper or receiver facility; rail transit system; rail transit facility; commercial motor vehicle; or pipeline; or a transportation-related automated system or network to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions or countermeasures to address security concerns.

[69 FR 28082, May 18, 2004, as amended at 70 FR 41599, July 19, 2005; 73 FR 72172, Nov. 26, 2008]

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, §1520.3 was amended by removing the definition of ''Security program'' effective November 16, 2009.

§1520.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the security of transportation.

(b) *Information constituting SSI.* Except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including—

(i) Any aircraft operator, airport operator, or fixed base operator security program, or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—

(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation, maritime, or rail transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation, maritime, or rail transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(iv) Any armed security officer procedures issued by TSA under 49 CFR part 1562.

(9) *Security screening information.* The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out aviation, maritime, or rail transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.* (i) Lists of the names or other identifying information that identify persons as—

(A) Having unescorted access to a secure area of an airport, a rail secure area, or a secure or restricted area of a maritime facility, port area, or vessel;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation, maritime, or rail infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or rail transportation system (including rail hazardous materials shippers and rail hazardous materials receivers) that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime

transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) *Loss of SSI designation.* TSA or the Coast Guard may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria set forth in paragraph (a) of this section.

[69 FR 28082, May 18, 2004, as amended at 70 FR 41599, July 19, 2005; 71 FR 30507, May 26, 2006; 73 FR 72172, Nov. 26, 2008]

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, §1520.5 was amended by revising paragraph (b)(1), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1520.5 Sensitive security information.

* * * * *

(b) * * *

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including any comments, instructions, or implementing guidance, including—

(i) Any aircraft operator, airport operator, fixed base operator, or air cargo security program, or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

* * * * *

§ 1520.7 Covered persons.

Persons subject to the requirements of part 1520 are:

(a) Each airport operator, aircraft operator, and fixed base operator subject to the requirements of subchapter C of this chapter, and each armed security officer under subpart B of part 1562.

(b) Each indirect air carrier, as defined in 49 CFR 1540.5.

(c) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.

(d) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107–295), 46 U.S.C. 70101 *et seq.*, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.*

(e) Each person performing the function of a computer reservation system or global distribution system for airline passenger information.

(f) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(g) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(h) DHS and DOT.

(i) Each person conducting research and development activities that relate to aviation or maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in §1520.11.

(k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

(m) Each person receiving SSI under §1520.15(d) or (e).

(n) Each railroad carrier, rail hazardous materials shipper, rail hazardous materials receiver, and rail

transit system subject to the requirements of part 1580 of this chapter.

[69 FR 28082, May 18, 2004, as amended at 70 FR 41600, July 19, 2005; 73 FR 72173, Nov. 26, 2008]

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, §1520.7 was amended by revising paragraph (b), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1520.7 Covered persons.

* * * * *

(b) Each indirect air carrier (IAC), as described in 49 CFR part 1548; each validation firm and its personnel, as described in 49 CFR 1522; and each certified cargo screening facility and its personnel, as described in 49 CFR 1549.

* * * * *

§ 1520.9 Restrictions on the disclosure of SSI.

(a) *Duty to protect information.* A covered person must—

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in §1520.13.

(5) Dispose of SSI as specified in §1520.19.

(b) *Unmarked SSI.* If a covered person receives a record containing SSI that is not marked as specified in §1520.13, the covered person must—

(1) Mark the record as specified in §1520.13; and

(2) Inform the sender of the record that the record must be marked as specified in §1520.13.

(c) *Duty to report unauthorized disclosure.* When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) *Additional Requirements for Critical Infrastructure Information.* In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

§ 1520.11 Persons with a need to know.

(a) *In general.* A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) *Federal, State, local, or tribal government employees, contractors, and grantees.* (1) A Federal, State, local, or tribal government employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties, on behalf or in defense of the interests of the Federal, State, local, or tribal government.

(2) A person acting in the performance of a contract with or grant from a

Federal, State, local, or tribal government agency has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) *Background check.* TSA or Coast Guard may make an individual's access to the SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI that are satisfactory to TSA or the Coast Guard.

(d) *Need to know further limited by the DHS or DOT.* For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

[69 FR 28082, May 18, 2004, as amended at 70 FR 1382, Jan. 7, 2005; 73 FR 72173, Nov. 26, 2008]

§ 1520.13 Marking SSI.

(a) *Marking of paper records.* In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) *Protective marking.* The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) *Distribution limitation statement.* The distribution limitation statement is:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ''need to know'', as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

(d) *Other types of records.* In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

§ 1520.15 SSI disclosed by TSA or the Coast Guard.

(a) *In general.* Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does TSA or the Coast Guard release such records to persons without a need to know.

(b) *Disclosure under the Freedom of Information Act and the Privacy Act.* If a record contains both SSI and information that is not SSI, TSA or the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) *Disclosures to committees of Congress and the General Accounting Office.* Nothing in this part precludes TSA or the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) *Disclosure in enforcement proceedings*—(1) *In general.* TSA or the Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of TSA or the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by TSA or the Coast Guard.

(2) *Security background check.* Prior to providing SSI to a person under paragraph (d)(1) of this section, TSA or the Coast Guard may require the individual or, in the case of an entity, the individuals representing the entity,

and their counsel, to undergo and satisfy, in the judgment of TSA or the Coast Guard, a security background check.

(e) *Other conditional disclosure.* TSA may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by TSA that disclosure of such records or information, subject to such limitations and restrictions as TSA may prescribe, would not be detrimental to transportation security.

(f) *Obligation to protect information.* When an individual receives SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under §1520.7 and is subject to the obligations of a covered person under this part.

(g) *No release under FOIA.* When TSA discloses SSI pursuant to paragraphs (b) through (e) of this section, TSA makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) *Disclosure of Critical Infrastructure Information.* Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

§ 1520.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

§ 1520.19 Destruction of SSI.

(a) *DHS.* Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function.

(b) *Other covered persons*—(1) *In general.* A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.

(2) *Exception.* Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

PART 1522—TSA-APPROVED VALIDATION FIRMS AND VALIDATORS (Eff. 11-16-09)

Subpart A—General

Sec.

Subpart B—TSA-Approved Validation Firms and Validators for the Certified Cargo Screening Program

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44932, 44935–44936, 44942, 46105.

SOURCE: 74 FR 47695, September 16, 2009, unless otherwise noted.

EFFECTIVE DATE NOTE: At 74 FR 47695, Sept. 16, 2009, part 1522 was added, effective Nov. 16, 2009.

Subpart A—General

§ 1522.1 Scope and terms used in this part.

(a) This part governs the use of TSA-approved validation firms and individual validators to assess whether certain persons regulated under this chapter are in compliance with this chapter.

(b) In addition to the terms in §§ 1500.3 and 1540.5 of this chapter, the following terms apply in this part:

Applicant means a firm that seeks to become a TSA-approved validation firm under this part.

Assessment means the physical inspections, records reviews, personnel interviews, and other procedures conducted by a validator to assess whether a person is in compliance with relevant requirements of a security program.

Conflict of interest means a situation in which the validation firm, the validator, or an individual assisting in the assessment, or the spouse or immediate family member of such person, has a relationship with, or an interest in, the person under assessment that may adversely affect the impartiality of the assessment. Examples of conflict of interest situations include, but are not limited to, any of the following:

(1) The validation firm is a parent company or subsidiary of the person under assessment, has a financial interest in the person under assessment, or has common management or organizational governance (for example, interlocking boards of directors) with the person under assessment.

(2) The validation firm, the validator, or an individual who will assist in conducting the assessment, or an immediate family member of such a validator or individual, is a creditor or debtor of the person under assessment.

(3) The validator, or an individual who will assist in conducting the assessment, or the spouse or immediate family member of such a person, is, or within the past two years has been, an employee, officer, or contractor of the person under assessment whose duties did not involve the operations being assessed.

(4) The validator, or an individual who will assist in conducting the assessment, or the spouse or immediate family member of such a person, is, or at any time has been, an individual, officer, or contractor of the person under assessment whose duties or responsibilities did involve the operations being assessed.

(5) The validator, or an individual who will assist in conducting the assessment, or the spouse or immediate family member of such a person, has a financial interest in the person under validation.

Firm means a business enterprise or other non-governmental organization, including a sole proprietorship, partnership, limited liability partnership, limited liability corporation, and a corporation.

National of the United States means a citizen of the United States, or a person who, though not a citizen, owes permanent allegiance to the United States, as defined in 8 U.S.C. 1101(a)(22), and includes American Samoa and Swains Island.

TSA-approved validation firm or *validation firm* means a firm that has been approved under this part to conduct an assessment under this chapter.

Validator means an individual assigned by the validation firm to be responsible for conducting a given assessment under this part.

§ 1522.3 Fraud and intentional falsification of records.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any application under this part.

(b) Any fraudulent or intentionally false entry in any record or report that is kept, made, or used to show compliance with this subchapter, or used to exercise any privilege under this part.

(c) Any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access medium, or identification medium issued or submitted under this part.

§ 1522.5 TSA inspection authority.

(a) Each validation firm and each validator must allow TSA, during normal business hours, in a reasonable manner, without advance notice, to

enter the facility and make any inspections or tests, including copying records, to—

(1) Determine compliance of a validation firm or validator with this chapter and 49 U.S.C. 114 and Subtitle VII, as amended; or

(2) Carry out TSA's statutory or regulatory authorities, including its authority to—

(i) Assess threats to transportation;

(ii) Enforce security-related regulations, directives, and requirements:

(iii) Inspect, maintain, and test the security of facilities, equipment, and systems;

(iv) Ensure the adequacy of security measures for the transportation of passengers and cargo;

(v) Oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

(vi) Review security plans; and

(vii) Carry out such other duties, and exercise such other powers, relating to transportation security as the Assistant Secretary of Homeland Security for the TSA considers appropriate, to the extent authorized by law.

(b) At the request of TSA, each validation firm and validator must provide evidence of compliance with this chapter, including copying records.

(c) TSA and DHS officials working with TSA may conduct inspections under this section without access media or identification media issued or approved by a validation firm or other person, except that the TSA and DHS officials will have identification media issued by TSA or DHS.

Subpart B—TSA-Approved Validation Firms and Validators for the Certified Cargo Screening Program

§ 1522.101 Applicability.

This subpart governs the use of TSA-approved validation firms and validators to assess whether certified cargo screening facilities (CCSFs), or facilities seeking to be approved as such, comply with the requirements of 49 CFR part 1549.

§ 1522.103 Requirements for validation firms.

In addition to the other requirements of this part, a validation firm must meet the following requirements to be approved to assess certified cargo screening facilities:

(a) *Resources.* The validation firm must have sufficient facilities, resources, and personnel to conduct the assessments.

(b) *Security Coordinator.* The validation firm must designate and use a Security Coordinator and at least one alternate Security Coordinator.

(1) The Security Coordinator and alternates must be senior employees or officers of the firm, and must be readily available during normal business hours.

(2) The Security Coordinator and designated alternates must serve as the validation firm's primary contact for security-related activities and communications with TSA.

(3) The Security Coordinator must immediately initiate corrective action for any instance of non-compliance by the validation firm with any applicable TSA security requirement.

(c) *Security Program.* The validation firm must obtain TSA approval of a security program and must implement the security program.

(d) *Personnel.* The validation firm must ensure that its personnel carry out the requirements of this chapter and the validation firm's security program.

(e) *Change in information.* (1) The validation firm must inform TSA, in a form and manner prescribed by TSA, of any change in the information required to be submitted by the validation firm to TSA under this part within seven days of the change.

(2) Changes included within the requirement of this paragraph include, but are not limited to, changes in the validation firm's address, phone number, or other contact information, the identity of the Security Coordinator or alternate, significant changes in ownership of the firm.

§ 1522.105 Adoption and implementation of the security program.

(a) *Security program required.* No person may operate as a validation firm

unless that person holds and carries out an approved security program under this part.

(b) *Content.* The validation firm standard security program together with approved alternate procedures and amendments that TSA has issued to that particular firm constitutes that firm's security program. Each security program under this part must—

(1) Provide for the security of aircraft, as well as that of persons and property traveling in air transportation, against acts of criminal violence and air piracy, and against the introduction into aircraft of any unauthorized explosive, incendiary, and other destructive substance or item;

(2) Describe the processes and procedures to be used to maintain current qualifications, credentials, or accreditations, training, and security threat assessments for relevant personnel;

(3) Describe the facilities, support personnel, and other resources to be used in conducting assessments; and

(4) Require that the validation firm designate and use a Security Coordinator and at least one alternate Security Coordinator.

(c) *Amendment requested by a validation firm or applicant.* A validation firm or applicant may file a request for an amendment to its security program with the TSA designated official at least 45 calendar days before the date it proposes for the amendment to become effective, unless the designated official allows a shorter period. Any validation firm may submit to TSA a group proposal for an amendment that is on behalf of it and other validation firms that co-sign the proposal.

(1) Within 30 calendar days after receiving a proposed amendment, the designated official, in writing, must either approve or deny the request to amend.

(2) An amendment to a validation firm's security program may be approved if the designated official determines that safety and the public interest will allow it, and if the proposed amendment provides the level of security required under this part.

(3) Within 30 calendar days after receiving a denial of the proposed amendment, the validation firm may petition TSA to reconsider the denial. A Petition for Reconsideration must be filed with the designated official.

(4) Upon receipt of a Petition for Reconsideration, the designated official must either approve the request to amend the security program or transmit the petition, along with any pertinent information, to TSA for reconsideration. TSA will make a determination on the petition within 30 calendar days of receipt by either directing the designated official to approve the amendment or by affirming the denial.

(d) *Amendment by TSA.* TSA may amend a security program in the interest of safety and the public interest, as follows:

(1) TSA must notify the validation firm, in writing, of the proposed amendment, fixing a period of not less than 30 calendar days within which the validation firm may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official must notify the validation firm of any amendment adopted or rescind the notice of amendment. If the amendment is adopted, it becomes effective not less than 30 calendar days after the validation firm receives the notice of amendment, unless the validation firm disagrees with the proposed amendment and petitions the TSA to reconsider, no later than 15 calendar days before the effective date of the amendment. The validation firm must send the petition for reconsideration to the designated official. A timely Petition for Reconsideration stays the effective date of the amendment.

(3) Upon receipt of a Petition for Reconsideration, the designated official must either amend or withdraw the notice of amendment, or transmit the Petition, together with any pertinent information, to TSA for reconsideration. TSA must make a determination on the Petition within 30 calendar days of receipt, either by directing the designated official to withdraw or amend the notice of amendment, or by affirming the notice of amendment.

(e) *Emergency Amendments.* (1) If TSA finds that there is an emergency requiring immediate action that makes compliance with the procedural requirements in this section contrary to

the public interest, the designated official may issue an emergency amendment, without the prior notice and comment procedures described in paragraph (d) of this section.

(2) The emergency amendment is effective without stay on the date the validation firm receives notification. TSA will incorporate in the notification a brief statement of the reasons and findings for the emergency amendment to be adopted.

(3) The validation firm may file a Petition for Reconsideration with TSA no later than 15 calendar days after TSA issues the emergency amendment. The certified cargo screening facility must send the Petition for Reconsideration to the designated official; however, the filing does not stay the effective date of the emergency amendment.

(f) *Availability.* Each validation firm having a security program must do the following:

(1) Maintain an original of the security program at its corporate office.

(2) Have accessible a complete copy, or the pertinent portions of its security program, or appropriate implementing instructions, at each office where it conducts validation services. An electronic version is adequate.

(3) Make a copy of the security program available for inspection upon the request of TSA.

(4) Restrict the distribution, disclosure, and availability of information contained in its security program to persons with a need to know, as described in part 1520 of this chapter.

(5) Refer requests for such information by other persons to TSA.

§ 1522.107 Application.

(a) *Initial application and approval.* Unless otherwise authorized by TSA, each applicant must apply for a security program and for approval to operate as a validation firm, in a form and a manner prescribed by TSA, not less than 90 calendar days before the applicant intends to begin operations. The application must be in writing and include the following:

(1) The firm's legal name; other names, including doing business as names; state of incorporation or licensing, if applicable; and tax identification number.

(2) The names of the senior officers or employees of the applicant who will serve as the Security Coordinator and alternates.

(3) A signed statement from each person listed in paragraph (a)(2) of this section stating whether he or she has been a senior manager or representative of any operator, whether or not a validation firm, that had its security program withdrawn by TSA.

(4) Copies of Government-issued identification of persons listed in paragraph (a)(2) of this section.

(5) The street address and e-mail address of the applicant.

(6) A statement acknowledging the requirement that all personnel of the applicant who are subject to training under the requirements of this part must successfully complete such training before performing security-related duties.

(7) Other information requested by TSA concerning security threat assessments.

(8) A statement acknowledging that all personnel of the applicant who must successfully complete a security threat assessment under the requirements of this part must do so before the applicant authorizes the personnel to perform duties under this part.

(b) *Standard security program.* After the Security Coordinator successfully completes a security threat assessment, TSA will provide to the applicant the validation firm standard security program, any security directives, and amendments to the security program and other alternative procedures that apply to validation firms. The applicant may either notify TSA that it accepts the standard security program or submit to TSA a proposed modified security program to the designated official for approval. The validation firm must also submit a supplement to the security program that specifies processes and procedures that the firm will use to maintain the qualification of its validators and its personnel assisting validators with assessments to the designated TSA official for approval. TSA will approve the security program under § 1522.109, or issue a written notice to modify under § 1522.109(b).

§ 1522.109 TSA review and approval.

(a) *Review.* TSA will review an application received under § 1522.107 to determine whether—

(1) The applicant has met the requirements of this part, the proposed security program, and any applicable Emergency Amendment and Security Directive;

(2) The applicant is able and willing to carry out the requirements of this part, its security program, and an applicable Emergency Amendment and Security Directive;

(3) The approval of such applicant's security program is not contrary to the interests of security and the public interest;

(4) The applicant has not held a security program that was withdrawn within the previous year, unless otherwise authorized by TSA; and

(5) TSA determines that the applicant is qualified to be a validation firm.

(b) *Notice*—(1) *Approval.* If an application is approved, TSA will send the applicant a written notice of approval of its security program, and approval to operate as a validation firm.

(2) *Commencement of operations.* A validation firm may commence operations when it has received approval under this section, and successfully completed training and security threat assessments for all relevant personnel.

(3) *Disapproval.* If an application is disapproved, TSA will serve a written notice of disapproval to the applicant. The notice of disapproval will include the basis of the disapproval of the application.

(c) *Duration of security program.* A security program approved under this section will remain effective until the end of the calendar month 12 months after the month it was approved or until the program has been surrendered or withdrawn, whichever is earlier.

§ 1522.111 Reconsideration of disapproval of an application.

(a) *Petition for reconsideration.* If TSA disapproves an application under section 1522.107, the applicant may seek reconsideration of the decision by submitting a written petition for reconsideration to the Assistant Secretary or his or her designee within 30 days of receiving the notice of disapproval. The written petition for reconsideration must include a statement and any supporting documentation explaining why the applicant believes the reason for disapproval is incorrect.

(b) *Review of petition.* Upon review of the petition for reconsideration, the Assistant Secretary or designee makes a determination on the petition by either affirming the disapproval of the application or approving the application. The Assistant Secretary or designee may request additional information from the applicant prior to rendering a decision. This disposition is a final agency action for purposes of 49 U.S.C. 46110.

§ 1522.113 Withdrawal of approval.

(a) *Basis for withdrawal of approval.* TSA may withdraw approval of a TSA-approved validation firm if the validation firm ceases to meet the standards for approval, fails to fulfill its responsibilities under this subpart, or if TSA determines that continued operation is contrary to safety and the public interest.

(b) *Notice of withdrawal of approval.* (1) Except as provided in paragraph (c) of this section, TSA will provide a written notice of proposed withdrawal of approval to the validation firm.

(2) The notice of proposed withdrawal of approval will include the basis for the withdrawal of approval.

(3) Unless the validation firm files a written petition for reconsideration under paragraph (d) of this section, the notice of proposed withdrawal of approval will become a final notice of withdrawal of approval 31 days after the validation firm's receipt of the notice of proposed withdrawal of approval.

(c) *Emergency notice of withdrawal of approval.* (1) If TSA finds that there is an emergency requiring immediate action with respect to a TSA-approved validation firm's ability to perform assessments, TSA may withdraw approval of that validation firm without prior notice.

(2) TSA will incorporate in the emergency notice of withdrawal of approval a brief statement of the reasons and findings for the withdrawal of approval.

(3) The emergency notice of withdrawal of approval is effective upon the TSA-approved validation firm's receipt of the notice. The validation firm may file a written petition for reconsideration under paragraph (d) of this section; however, this petition does not stay the effective date of the emergency notice of withdrawal of approval.

(d) *Petition for reconsideration.* A validation firm may seek reconsideration of the withdrawal of approval by submitting a written petition for reconsideration to the Assistant Secretary or designee within 30 days of receiving the notice of withdrawal of approval. The filing of a petition for reconsideration does not stay the effective date of the withdrawal pending the reconsideration.

(e) *Review of petition.* Upon review of the written petition for reconsideration, the Assistant Secretary or designee makes a determination on the petition by either affirming or withdrawing the notice of withdrawal of approval. The Assistant Secretary or designee may request additional information from the validation firm prior to rendering a decision. This disposition is a final decision for purposes of review under 49 U.S.C. 46110.

§ 1522.115 Renewal of TSA approval.

(a) *Application.* Every 12 months, computed from the date of initial approval under § 1522.107, or more frequently as required by TSA, each validation firm must apply, in a form and manner prescribed by TSA, for renewal of approval of its security program, and of approval to operate as a validation firm. If the validation firm submits the information in the month before or after it is due, the validation firm is considered to have submitted the information in the month it is due. If the validation firm timely submits its application for review of approval under this section, the validation firm may continue to conduct assessments under this subpart unless and until TSA denies the application.

(b) *Content.* In addition to any other information required by TSA, the validation firm must submit the following information to TSA when applying for renewal:

(1) If required, evidence that the validators and other individuals of the validation firm with responsibilities for participating in assessments have successfully completed the initial training under § 1522.119(a) and any recurrent training described in § 1522.119(b).

(2) Evidence that the individual validators with responsibilities for conducting assessments continue to be certified or accredited by an organization that TSA recognizes as qualified to certify or accredit a validator.

(3) A statement signed by a senior officer or employee of the validation firm attesting that the firm has reviewed and ensures the continuing accuracy of the contents of its initial application for a security program, subsequent renewal applications, or other submissions to TSA confirming a change of information and noting the date such applications and submissions were made to TSA, including the following certification:

> [Name of validation firm] (hereinafter ''the validation firm'') has adopted and is currently carrying out a security program in accordance with the Transportation Security Regulations as originally approved on [Insert date of TSA initial approval]. In accordance with TSA regulations, the validation firm has notified TSA of any new or changed information required for the validation firm's initial security program. If new or changed information is being submitted to TSA as part of this application for reapproval, that information is stated in this filing.
>
> The validation firm understands that intentional falsification of certification may be subject to both civil and criminal penalties under 49 CFR part 1540 and 18 U.S.C. 1001. Failure to notify TSA of any new or changed information required for initial approval of the validation firm's security program in a timely fashion and in a form acceptable to TSA may result in withdrawal by TSA of approval of the validation firm's security program.

(c) *Renewal.* TSA will renew approval of the security program and the validation firm's authority to conduct assessments if TSA determines that—

(1) The validation firm has met the requirements of this chapter, its security program, and any Security Directive; and

(2) The renewal of approval of the validation firm's security program, and

of the approval to operate as a validation firm, is not contrary to the interests of security or the public interest.

(d) *Effective.* The renewal of approval issued pursuant to this section will remain effective until the end of the calendar month 12 months after the month it was approved or until the program has been surrendered or withdrawn, whichever is earlier.

(e) *Withdrawal.* If a validation firm fails to comply with the requirements of this section, TSA may withdraw approval of the validation firm under § 1522.113.

§ 1522.117 Qualifications of validators.

(a) Each assessment conducted under this subpart must be conducted by a validator who meets the following requirements:

(1) He or she must be a citizen or national of the United States or be an alien lawfully admitted for permanent residence.

(2) He or she must meet the requirements of paragraph (a)(2)(i) or (ii) of this section.

(i) He or she must hold a certification or accreditation from an organization that TSA recognizes as qualified to certify or accredit a validator for assessments and must have at least five years of experience in inspection or validating compliance with State or Federal regulations in the security industry, the aviation industry, or government programs. The five years of experience must have been obtained within 10 years of the date of the application.

(ii) He or she must have at least five years experience as an inspector for a Federal or State government agency performing inspections similar to the inspections called for in this subpart and part 1549. The five years of experience must have been obtained within 10 years of the date of the application.

(3) The validator must have three professional references that address his or her abilities in inspection, validation, and written communications.

(4) The validator must have sufficient knowledge of the rules, regulations, policies, security programs, directives, and orders, pertaining to the certified cargo screening program (CCSP).

(5) The validator must have the ability to apply the concepts, principles, and methods of compliance with the requirements of the certified cargo screening program to include assessment, inspection, investigation, and reporting of compliance with the certified cargo screening program.

(b) Each validator and each individual who assists in conducting assessments must successfully undergo a security threat assessment as required under § 1522.121.

§ 1522.119 Training.

(a) *Initial training.* The validation firm must ensure that its validators and individuals who will assist in conducting assessments have completed the initial training prescribed by TSA before conducting any assessment under this subpart.

(b) *Recurrent training.* The validation firm must ensure that each validator and each individual assisting in conducting assessments under this subpart completes the recurrent training prescribed by TSA not later than 12 months after the validator's or individual's most recent TSA-prescribed training. If the validator or individual completes the recurrent training in the month before or the month after it is due, he or she is considered to have taken it in the month it is due.

(c) *Content.* The training required by this section will include coverage of the applicable provisions of this chapter, including this part, part 1520, and § 1540.105.

§ 1522.121 Security threat assessments for personnel of TSA-approved validation firms.

Each of the following must successfully complete a security threat assessment or comparable security threat assessment described in part 1540, subpart C of this chapter:

(a) Each individual who supervises validators or individuals who will assist validators.

(b) The validation firm's validator authorized to perform assessment services under this subpart.

(c) The validation firm's Security Coordinator and alternates.

(d) Each individual who will assist the validator in conducting assessments.

§ 1522.123 Conduct of assessments.

(a) *Standards for assessment.* Each validator must assess, in a form and manner prescribed by TSA, whether the person seeking to operate or operating as a certified cargo screening facility is in compliance with 49 CFR part 1549. The validator may be assisted by other individuals; however, the validator is directly responsible for the assessment and must sign the assessment report.

(b) *Conflict of interest.* A validator may not conduct an assessment for which there exists a conflict of interest as defined in § 1552.1.

(c) *Immediate notification to TSA.* If during the course of an assessment, the validator believes that there is or may be an instance of noncompliance with TSA requirements that presents an imminent threat to transportation security or public safety, he or she must report the instance immediately to the Security Coordinator, and the Security Coordinator must report the instance immediately to TSA.

(d) *No authorization to take remedial or disciplinary action.* Neither the validation firm nor the validator is authorized to require any remedial action by, or to take any disciplinary or enforcement action against, the facility under assessment.

(e) *Prohibition on consecutive assessments.* Unless otherwise authorized by TSA, a validation firm must not conduct more than two consecutive assessments of a person seeking approval, or renewal of approval, to operate a certified cargo screening facility.

§ 1522.125 Protection of information.

(a) *Sensitive Security Information.* Each validation firm must comply with the requirements in 49 CFR part 1520 regarding the handling and protection of Sensitive Security Information (SSI).

(b) *Non-disclosure of proprietary information.* Unless explicitly authorized by TSA, no validation firm, or any of its officers, Security Coordinators, validators, or employees, or individuals assisting in validations, may make an unauthorized release nor disseminate any information that TSA or an entity being assessed indicates is proprietary information.

§ 1522.127 Assessment report.

(a) Each validator must prepare and submit to TSA a written assessment report, in a manner and form prescribed by TSA, within 30 calendar days of completing each assessment.

(b) The assessment report must include the following information, in addition to any other information otherwise required by TSA:

(1) A description of the facilities, equipment, systems, processes, and/or procedures that were assessed and any other information as determined by TSA.

(2) The validator's assessment regarding the facility's compliance with TSA requirements, including all elements of the applicable security program.

(3) Signed attestation by the individual validator with responsibility for the assessment that no conflicts of interest existed with regard to the assessment and that the assessment was conducted impartially, professionally, and consistent with the standards set forth by TSA.

§ 1522.129 Recordkeeping requirements.

(a) Each validation firm must maintain records demonstrating compliance with all statutes, regulations, directives, orders, and security programs that apply to operation as a validation firm, including the records listed below.

(b) Each validation firm must retain the following records for 180 days after the individual is no longer employed by the validation firm or is no longer acting as the firm's agent.

(1) Records of all training and instruction given to each individual under the requirements of this subpart.

(2) Records demonstrating that the validation firm has complied with the security threat assessment provisions of § 1522.121.

(3) Records about the qualifications of validators it uses to conduct assessments under this subpart.

(c) Each validation firm must retain the following records until completion of the validation firm's next review under §1522.115, after which the records may be destroyed unless TSA instructs the validation firm to retain the records for a longer period.

(1) Copies of all applications for approval, or renewal of approval, by TSA to operate as a validation firm under part 1522.

(2) Copies of TSA's approval and renewals of approval as required by part 1522.

(d) Each validation firm must retain assessment reports and copies of back-up documentation supporting each assessment report submitted to TSA for 42 months after the assessment.

SUBCHAPTER C—CIVIL AVIATION SECURITY

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

Subpart A—General

Sec.

Subpart B—Responsibilities of Passengers and Other Individuals and Persons

Subpart C—Security Threat Assessments

Subpart D—Responsibilities of Holders of TSA-Approved Security Programs

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

SOURCE: 67 FR 8353, Feb. 22, 2002, unless otherwise noted.

Subpart A—General

§ 1540.1 Applicability of this subchapter and this part.

This subchapter and this part apply to persons engaged in aviation-related activities.

§ 1540.3 Delegation of authority.

(a) Where the Administrator is named in this subchapter as exercising authority over a function, the authority is exercised by the Administrator or the Deputy Administrator, or any individual formally designated to act as the Administrator or the Deputy Administrator.

(b) Where TSA or the designated official is named in this subchapter as exercising authority over a function, the authority is exercised by the official designated by the Administrator to perform that function.

§ 1540.5 Terms used in this subchapter.

In addition to the terms in part 1500 of this chapter, the following terms are used in this subchapter:

Air operations area (AOA) means a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas, for use by aircraft regulated under 49 CFR part 1544 or 1546, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the secured area.

Aircraft operator means a person who uses, causes to be used, or authorizes to be used an aircraft, with or without the right of legal control (as owner, lessee, or otherwise), for the purpose of air navigation including the piloting of aircraft, or on any part of the surface of an airport. In specific parts or sections of this subchapter, ''aircraft operator'' is used to refer to specific types of operators as described in those parts or sections.

Airport operator means a person that operates an airport serving an aircraft operator or a foreign air carrier required to have a security program under part 1544 or 1546 of this chapter.

Airport security program means a security program approved by TSA under §1542.101 of this chapter.

Airport tenant means any person, other than an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter, that has an agreement with the airport operator to conduct business on airport property.

Airport tenant security program means the agreement between the airport operator and an airport tenant that specifies the measures by which the tenant will perform security functions, and approved by TSA, under §1542.113 of this chapter.

Approved, unless used with reference to another person, means approved by TSA.

Cargo means property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. Aircraft operator security programs further define the term ''cargo.''

Checked baggage means property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during flight. Accompanied commercial courier consignments are not classified as checked baggage.

Escort means to accompany or monitor the activities of an individual who does not have unescorted access authority into or within a secured area or SIDA.

Exclusive area means any portion of a secured area, AOA, or SIDA, including individual access points, for which an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter has assumed responsibility under §1542.111 of this chapter.

Exclusive area agreement means an agreement between the airport operator and an aircraft operator or a foreign air carrier that has a security program under parts 1544 or 1546 of this chapter that permits such an aircraft operator or foreign air carrier to assume responsibility for specified security measures in accordance with §1542.111 of this chapter.

FAA means the Federal Aviation Administration.

Flightcrew member means a pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time.

Indirect air carrier (IAC) means any person or entity within the United States not in possession of an FAA air carrier operating certificate, that 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. This does not include the United States Postal Service (USPS) or its representative while acting on the behalf of the USPS.

Loaded firearm means a firearm that has a live round of ammunition, or any component thereof, in the chamber or cylinder or in a magazine inserted in the firearm.

Passenger seating configuration means the total maximum number of seats for which the aircraft is type certificated that can be made available for passenger use aboard a flight, regardless of the number of seats actually installed, and includes that seat in certain aircraft that may be used by a representative of the FAA to conduct flight checks but is available for revenue purposes on other occasions.

Private charter means any aircraft operator flight—

(1) For which the charterer engages the total passenger capacity of the aircraft for the carriage of passengers; the passengers are invited by the charterer; the cost of the flight is borne entirely by the charterer and not directly or indirectly by any individual passenger; and the flight is not advertised to the public, in any way, to solicit passengers.

(2) For which the total passenger capacity of the aircraft is used for the purpose of civilian or military air movement conducted under contract with the Government of the United States or the government of a foreign country.

Public charter means any charter flight that is not a private charter.

Scheduled passenger operation means an air transportation operation (a flight) from identified air terminals at a set time, which is held out to the public and announced by timetable or schedule, published in a newspaper, magazine, or other advertising medium.

Screening function means the inspection of individuals and property for weapons, explosives, and incendiaries.

Screening location means each site at which individuals or property are inspected for the presence of weapons, explosives, or incendiaries.

Secured area means a portion of an airport, specified in the airport security program, in which certain security measures specified in part 1542 of this chapter are carried out. This area is where aircraft operators and foreign air carriers that have a security program under part 1544 or 1546 of this chapter enplane and deplane passengers and sort and load baggage and any adjacent areas that are not separated by adequate security measures.

Security Identification Display Area (SIDA) means a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.

Sterile area means a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under part 1544 of this chapter or a foreign air carrier under part 1546 of this chapter, through the screening of persons and property.

Unescorted access authority means the authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under part 1542, 1544, or 1546 of this chapter, to individuals to gain entry to, and be present without an escort in, secured areas and SIDA's of airports.

Unescorted access to cargo means the authority granted by an aircraft operator or IAC to individuals to have access to air cargo without an escort.

[67 FR 8353, Feb. 22, 2002, as amended at 67 FR 8209, Feb. 22, 2002; 71 FR 30507, May 26, 2006]

EFFECTIVE DATE NOTE: At 74 FR 47700, Sept. 16, 2009, §1540.5 was amended by adding the definiions of ''certified cargo screening program'', ''certified cargo screening facility'', and ''standard security program'' in alphabetical order, effective November 16, 2009. For the convenience of the user, the added text is set forth as follows:

§ 1540.5 Terms used in this subchapter.

* * * * *

Certified cargo screening program (CCSP) means the program under which facilities are authorized to screen cargo to be offered for transport on certain passenger aircraft in accordance with 49 CFR part 1549.

Certified cargo screening facility (CCSF) means a facility certified by TSA to screen air cargo in accordance with part 1549. As used in this subchapter, ''certified cargo screening facility'' refers to the legal entity that operates a CCSF at a particular location.

* * * * *

Standard security program means a security program issued by TSA that serves as a baseline for a particular type of operator. If TSA has issued a standard security program for a particular type of operator, unless otherwise authorized by TSA, each operator's security program consists of the standard security program together with any amendments and alternative procedures approved or accepted by TSA.

* * * * *

Subpart B—Responsibilities of Passengers and Other Individuals and Persons

§ 1540.101 Applicability of this subpart.

This subpart applies to individuals and other persons.

§ 1540.103 Fraud and intentional falsification of records.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any application for any security program, access medium, or identification medium, or any amendment thereto, under this subchapter.

(b) Any fraudulent or intentionally false entry in any record or report that

is kept, made, or used to show compliance with this subchapter, or exercise any privileges under this subchapter.

(c) Any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access medium, or identification medium issued under this subchapter.

§ 1540.105 Security responsibilities of employees and other persons.

(a) No person may:

(1) Tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under this subchapter.

(2) Enter, or be present within, a secured area, AOA, SIDA or sterile area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas.

(3) Use, allow to be used, or cause to be used, any airport-issued or airport-approved access medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in secured areas, AOA's, or SIDA's in any other manner than that for which it was issued by the appropriate authority under this subchapter.

(b) The provisions of paragraph (a) of this section do not apply to conducting inspections or tests to determine compliance with this part or 49 U.S.C. Subtitle VII authorized by:

(1) TSA, or

(2) The airport operator, aircraft operator, or foreign air carrier, when acting in accordance with the procedures described in a security program approved by TSA.

§ 1540.107 Submission to screening and inspection.

(a) No individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft under this subchapter.

(b) An individual must provide his or her full name, as defined in §1560.3 of this chapter, date of birth, and gender when—

(1) The individual, or a person on the individual's behalf, makes a reservation for a covered flight, as defined in §1560.3 of this chapter, or

(2) The individual makes a request for authorization to enter a sterile area.

(c) An individual may not enter a sterile area or board an aircraft if the individual does not present a verifying identity document as defined in §1560.3 of this chapter, when requested for purposes of watch list matching under §1560.105(c), unless otherwise authorized by TSA on a case-by-case basis.

[73 FR 64061, Oct. 28, 2008]

§ 1540.109 Prohibition against interference with screening personnel.

No person may interfere with, assault, threaten, or intimidate screening personnel in the performance of their screening duties under this subchapter.

§ 1540.111 Carriage of weapons, explosives, and incendiaries by individuals.

(a) *On an individual's person or accessible property—prohibitions.* Except as provided in paragraph (b) of this section, an individual may not have a weapon, explosive, or incendiary, on or about the individual's person or accessible property—

(1) When performance has begun of the inspection of the individual's person or accessible property before entering a sterile area, or before boarding an aircraft for which screening is conducted under this subchapter;

(2) When the individual is entering or in a sterile area; or

(3) When the individual is attempting to board or onboard an aircraft for which screening is conducted under §§1544.201, 1546.201, or 1562.23 of this chapter.

(b) *On an individual's person or accessible property—permitted carriage of a weapon.* Paragraph (a) of this section does not apply as to carriage of firearms and other weapons if the individual is one of the following:

(1) Law enforcement personnel required to carry a firearm or other

weapons while in the performance of law enforcement duty at the airport.

(2) An individual authorized to carry a weapon in accordance with §§ 1544.219, 1544.221, 1544.223, 1546.211, or subpart B of part 1562 of this chapter.

(3) An individual authorized to carry a weapon in a sterile area under a security program.

(c) *In checked baggage.* A passenger may not transport or offer for transport in checked baggage or in baggage carried in an inaccessible cargo hold under § 1562.23 of this chapter:

(1) Any loaded firearm(s).

(2) Any unloaded firearm(s) unless—

(i) The passenger declares to the aircraft operator, either orally or in writing, before checking the baggage, that the passenger has a firearm in his or her bag and that it is unloaded;

(ii) The firearm is unloaded;

(iii) The firearm is carried in a hard-sided container; and

(iv) The container in which it is carried is locked, and only the passenger retains the key or combination.

(3) Any unauthorized explosive or incendiary.

(d) *Ammunition.* This section does not prohibit the carriage of ammunition in checked baggage or in the same container as a firearm. Title 49 CFR part 175 provides additional requirements governing carriage of ammunition on aircraft.

[67 FR 8353, Feb. 22, 2002, as amended at 67 FR 41639, June 19, 2002; 70 FR 41600, July 19, 2005; 71 FR 30507, May 26, 2006]

§ 1540.113 Inspection of airman certificate.

Each individual who holds an airman certificate, medical certificate, authorization, or license issued by the FAA must present it for inspection upon a request from TSA.

§ 1540.115 Threat assessments regarding citizens of the United States holding or applying for FAA certificates, ratings, or authorizations.

(a) *Applicability.* This section applies when TSA has determined that an individual who is a United States citizen and who holds, or is applying for, an airman certificate, rating, or authorization issued by the Administrator, poses a security threat.

(b) *Definitions.* The following terms apply in this section:

Administrator means the Administrator of the Transportation Security Administration.

Assistant Administrator means the Assistant Administrator for Intelligence for TSA.

Date of service means—

(1) The date of personal delivery in the case of personal service;

(2) The mailing date shown on the certificate of service;

(3) The date shown on the postmark if there is no certificate of service; or

(4) Another mailing date shown by other evidence if there is no certificate of service or postmark.

Deputy Administrator means the officer next in rank below the Administrator.

FAA Administrator means the Administrator of the Federal Aviation Administration.

Individual means an individual whom TSA determines poses a security threat.

(c) *Security threat.* An individual poses a security threat when the individual is suspected of posing, or is known to pose—

(1) A threat to transportation or national security;

(2) A threat of air piracy or terrorism;

(3) A threat to airline or passenger security; or

(4) A threat to civil aviation security.

(d) *Representation by counsel.* The individual may, if he or she so chooses, be represented by counsel at his or her own expense.

(e) *Initial Notification of Threat Assessment*—(1) *Issuance.* If the Assistant Administrator determines that an individual poses a security threat, the Assistant Administrator serves upon the individual an Initial Notification of Threat Assessment and serves the determination upon the FAA Administrator. The Initial Notification includes—

(i) A statement that the Assistant Administrator personally has reviewed the materials upon which the Initial Notification was based; and

(ii) A statement that the Assistant Administrator has determined that the individual poses a security threat.

(2) *Request for Materials.* Not later than 15 calendar days after the date of service of the Initial Notification, the individual may serve a written request for copies of the releasable materials upon which the Initial Notification was based.

(3) *TSA response.* Not later than 30 calendar days, or such longer period as TSA may determine for good cause, after receiving the individual's request for copies of the releasable materials upon which the Initial Notification was based, TSA serves a response. TSA will not include in its response any classified information or other information described in paragraph (g) of this section.

(4) *Reply.* The individual may serve upon TSA a written reply to the Initial Notification of Threat Assessment not later than 15 calendar days after the date of service of the Initial Notification, or the date of service of TSA's response to the individual's request under paragraph (e)(2) if such a request was served. The reply may include any information that the individual believes TSA should consider in reviewing the basis for the Initial Notification.

(5) *TSA final determination.* Not later than 30 calendar days, or such longer period as TSA may determine for good cause, after TSA receives the individual's reply, TSA serves a final determination in accordance with paragraph (f) of this section.

(f) *Final Notification of Threat Assessment*—(1) *In general.* The Deputy Administrator reviews the Initial Notification, the materials upon which the Initial Notification was based, the individual's reply, if any, and any other materials or information available to him.

(2) *Review and Issuance of Final Notification.* If the Deputy Administrator determines that the individual poses a security threat, the Administrator reviews the Initial Notification, the materials upon which the Initial Notification was based, the individual's reply, if any, and any other materials or information available to him. If the Administrator determines that the individual poses a security threat, the Administrator serves upon the individual a Final Notification of Threat Assessment and serves the determination upon the FAA Administrator. The Final Notification includes a statement that the Administrator personally has reviewed the Initial Notification, the individual's reply, if any, and any other materials or information available to him, and has determined that the individual poses a security threat.

(3) *Withdrawal of Initial Notification.* If the Deputy Administrator does not determine that the individual poses a security threat, or upon review, the Administrator does not determine that the individual poses a security threat, TSA serves upon the individual a Withdrawal of the Initial Notification and provides a copy of the Withdrawal to the FAA Administrator.

(g) *Nondisclosure of certain information.* In connection with the procedures under this section, TSA does not disclose to the individual classified information, as defined in Executive Order 12968 section 1.1(d), and reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

[68 FR 3761, Jan. 24, 2003, as amended at 68 FR 49721, Aug. 19, 2003]

§ 1540.117 Threat assessments regarding aliens holding or applying for FAA certificates, ratings, or authorizations.

(a) Applicability. This section applies when TSA has determined that an individual who is not a citizen of the United States and who holds, or is applying for, an airman certificate, rating, or authorization issued by the FAA Administrator, poses a security threat.

(b) *Definitions.* The following terms apply in this section:

Assistant Administrator means the Assistant Administrator for Intelligence for TSA.

Date of service means—

(1) The date of personal delivery in the case of personal service;

(2) The mailing date shown on the certificate of service;

(3) The date shown on the postmark if there is no certificate of service; or

(4) Another mailing date shown by other evidence if there is no certificate of service or postmark.

Deputy Administrator means the officer next in rank below the Administrator.

FAA Administrator means the Administrator of the Federal Aviation Administration.

Individual means an individual whom TSA determines poses a security threat.

(c) *Security threat.* An individual poses a security threat when the individual is suspected of posing, or is known to pose—

(1) A threat to transportation or national security;

(2) A threat of air piracy or terrorism;

(3) A threat to airline or passenger security; or

(4) A threat to civil aviation security.

(d) *Representation by counsel.* The individual may, if he or she so chooses, be represented by counsel at his or her own expense.

(e) *Initial Notification of Threat Assessment*—(1) *Issuance.* If the Assistant Administrator determines that an individual poses a security threat, the Assistant Administrator serves upon the individual an Initial Notification of Threat Assessment and serves the determination upon the FAA Administrator. The Initial Notification includes—

(i) A statement that the Assistant Administrator personally has reviewed the materials upon which the Initial Notification was based; and

(ii) A statement that the Assistant Administrator has determined that the individual poses a security threat.

(2) *Request for materials.* Not later than 15 calendar days after the date of service of the Initial Notification, the individual may serve a written request for copies of the releasable materials upon which the Initial Notification was based.

(3) *TSA response.* Not later than 30 calendar days, or such longer period as TSA may determine for good cause, after receiving the individual's request for copies of the releasable materials upon which the Initial Notification was based, TSA serves a response. TSA will not include in its response any classified information or other information described in paragraph (g) of this section.

(4) *Reply.* The individual may serve upon TSA a written reply to the Initial Notification of Threat Assessment not later than 15 calendar days after the date of service of the Initial Notification, or the date of service of TSA's response to the individual's request under paragraph (e)(2) if such a request was served. The reply may include any information that the individual believes TSA should consider in reviewing the basis for the Initial Notification.

(5) *TSA final determination.* Not later than 30 calendar days, or such longer period as TSA may determine for good cause, after TSA receives the individual's reply, TSA serves a final determination in accordance with paragraph (f) of this section.

(f) *Final Notification of Threat Assessment*—(1) *In general.* The Deputy Administrator reviews the Initial Notification, the materials upon which the Initial Notification was based, the individual's reply, if any, and any other materials or information available to him.

(2) *Issuance of Final Notification.* If the Deputy Administrator determines that the individual poses a security threat, the Deputy Administrator serves upon the individual a Final Notification of Threat Assessment and serves the determination upon the FAA Administrator. The Final Notification includes a statement that the Deputy Administrator personally has reviewed the Initial Notification, the individual's reply, if any, and any other materials or information available to him, and has determined that the individual poses a security threat.

(3) *Withdrawal of Initial Notification.* If the Deputy Administrator does not determine that the individual poses a security threat, TSA serves upon the individual a Withdrawal of the Initial Notification and provides a copy of the Withdrawal to the FAA Administrator.

(g) *Nondisclosure of certain information.* In connection with the procedures

under this section, TSA does not disclose to the individual classified information, as defined in Executive Order 12968 section 1.1(d), and TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

[68 FR 3768, Jan. 24, 2003]

Subpart C—Security Threat Assessments

SOURCE: 72 FR 3592, Jan. 25, 2007, unless otherwise noted.

EFFECTIVE DATE NOTE: At 74 FR 47700, Sept. 16, 2009, subpart C was revised, effective November 16, 2009. The new subpart appears after the text of this subpart.

§ 1540.201 Applicability and terms used in this subpart.

(a) This subpart includes the procedures that certain aircraft operators, foreign air carriers, and indirect air carriers must use to have security threat assessments done on certain individuals pursuant to 49 CFR 1544.228, 1546.213, 1548.7, 1548.15, and 1548.16. This subpart applies to the following:

(1) Each aircraft operator operating under a full program or full all-cargo program described in 49 CFR 1544.101(a) or (h).

(2) Each foreign air carrier operating under a program described in 49 CFR 1546.101(a), (b), or (e).

(3) Each indirect air carrier operating under a security program described in 49 CFR part 1548.

(4) Each applicant applying for unescorted access to cargo under one of the programs described in (a)(1) through (a)(3) of this section.

(5) Each proprietor, general partner, officer, director, or owner of an indirect air carrier as described in 49 CFR 1548.16.

(b) For purposes of this subpart—

Applicant means the individuals listed in paragraph (a)(4) and (a)(5) of this section.

Operator means an aircraft operator, foreign air carrier, and indirect air carrier listed in paragraphs (a)(1) through (a)(3) of this section.

(c) An applicant poses a security threat under this subpart when TSA determines that he or she is known to pose or suspected of posing a threat—

(1) To national security;

(2) To transportation security; or

(3) Of terrorism.

[72 FR 3592, Jan. 25, 2007; 72 FR 14049, Mar. 26, 2007]

§ 1540.203 Operator responsibilities.

(a) Each operator subject to this subpart must ensure that each applicant described in § 1540.201(a)(4) and (a)(5) completes the Security Threat Assessment described in this section.

(b) Each operator must:

(1) Authenticate the identity of the applicant by—

(i) Reviewing two forms of identification, one of which must be a government-issued picture identification; or

(ii) Other means approved by TSA.

(2) Submit to TSA a Security Threat Assessment application for each applicant that is signed by the applicant and that includes:

(i) Legal name, including first, middle, and last; any applicable suffix; and any other names used previously.

(ii) Current mailing address, including residential address if it differs from the current mailing address, and all other residential addresses for the previous five years, and e-mail address, if the applicant has an e-mail address.

(iii) Date and place of birth.

(iv) Social security number (submission is voluntary, although failure to provide it may delay or prevent completion of the threat assessment).

(v) Gender.

(vi) Country of citizenship, and if naturalized in the United States, date of naturalization and certificate number.

(vii) Alien registration number, if applicable.

(viii) The following statement reading:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 49 U.S.C. 5103a. *Purpose:* This information is needed to verify your identity and to conduct a Security Threat Assessment to evaluate your suitability for completing the functions required by this position. Failure to furnish your SSN may result in delays in processing your application, but will not prevent completion of your Security Threat Assessment. Furnishing the other information is also voluntary; however, failure

to provide it may delay or prevent the completion of your Security Threat Assessment, without which you may not be granted authorization to have unescorted access to air cargo subject to TSA security requirements. *Routine Uses:* Routine uses of this information include disclosure to TSA contractors or other agents who are providing services relating to the Security Threat Assessments; to appropriate governmental agencies for law enforcement or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement. For further information, please consult DHS/TSA 002 Transportation Security Threat Assessment System.

The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact, on this application can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of authorization or in the case of parties regulated under this section, removal of authorization to operate under this chapter, if applicable.

(3) Retain the applicant's signed Security Threat Assessment application, and any communications with TSA regarding the applicant's application, for 180 days following the end of the applicant's service to the operator.

(c) Records under this section may include electronic documents with electronic signature or other means of personal authentication, where accepted by TSA.

[72 FR 3592, Jan. 25, 2007; 72 FR 14050, Mar. 26, 2007]

§ 1540.205 Procedures for security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA conducts includes an intelligence-related check and a final disposition.

(b) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1540.203(b);

(2) Searches domestic and international Government databases to determine if an applicant meets the requirements of 49 CFR 1540.201(c) or to confirm an applicant's identity; and

(3) Adjudicates the results in accordance with 49 CFR 1540.201(c).

(c) *Final disposition.* Following completion of the procedures described in paragraph (b), the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the applicant and the operator, if TSA determines that the applicant meets the security threat assessment standards in 49 CFR 1540.201(c).

(2) TSA serves an Initial Determination of Threat Assessment on the applicant and the operator, if TSA determines that the applicant does not meet the security threat assessment standards in 49 CFR 1540.201(c). The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.9; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) If the applicant does not appeal the Initial Determination of Threat Assessment, TSA serves a Final Determination of Threat Assessment on the operator and the applicant.

(d) *Withdrawal by TSA.* TSA serves a Withdrawal of the Initial Determination of Threat Assessment on the applicant and a Determination of No Security Threat on the operator, if the appeal results in a determination that the applicant does not pose a security threat.

[72 FR 3588, Jan. 25, 2007; 72 FR 5633, Feb. 7, 2007; 72 FR 14050, Mar. 26, 2007]

§ 1540.207 [Reserved]

§ 1540.209 Security threat assessment fee.

(a) *Imposition of fees.* The fee of $28 is required for TSA to conduct a security threat assessment for an applicant.

(b) *Remittance of fees.* (1) The fee required under this subpart must be remitted to TSA, in a form and manner acceptable to TSA, each time the applicant or an aircraft operator, foreign air carrier, or indirect air carrier submits the information required under § 1540.203 to TSA.

(2) Fees remitted to TSA under this subpart must be payable to the ''Transportation Security Administration'' in U.S. currency and drawn on a U.S. bank.

(3) TSA will not issue any fee refunds, unless a fee was paid in error.

EFFECTIVE DATE NOTE: At 74 FR 47700, Sept. 16, 2009, subpart C was revised, effective Nov. 16, 2009. For the convenience of the user, the revised text is set forth as follows:

Subpart C—Security Threat Assessments

§ 1540.201 Applicability and terms used in this subpart.

(a) This subpart includes the procedures that certain aircraft operators, foreign air carriers, indirect air carriers, certified cargo screening facilities, and TSA-approved validation firms must use to have security threat assessments performed on certain individuals pursuant to 49 CFR 1522.121, 1544.228, 1546.213, 1548.7, 1548.15, 1548.16, and 1549.113. This subpart applies to the following:

(1) Each aircraft operator operating under a full program or full all-cargo program described in 49 CFR 1544.101(a) or (h).

(2) Each foreign air carrier operating under a program described in 49 CFR 1546.101(a), (b), or (e).

(3) Each indirect air carrier operating under a security program described in 49 CFR part 1548.

(4) Each applicant applying for unescorted access to cargo under one of the programs described in (a)(1) through (a)(3) of this section.

(5) Each proprietor, general partner, officer, director, or owner of an indirect air carrier as described in 49 CFR 1548.16.

(6) Each certified cargo screening facility described in 49 CFR part 1549.

(7) Each individual a certified cargo screening facility authorizes to perform screening or supervise screening.

(8) Each individual the certified cargo screening facility authorizes to have unescorted access to cargo at any time from the time it is screened until the time it is tendered to an indirect air carrier under 49 CFR part 1548, an aircraft operator under part 1544, or a foreign air carrier under part 1546.

(9) The senior manager or representative of its facility in control of the operations of a certified cargo screening facility under 49 CFR part 1549.

(10) Each TSA-approved validation firm for the certified cargo screening program described in 49 CFR part 1522 subpart B.

(11) Each individual of the TSA-approved validation firm under 49 CFR part 1522 subpart B who supervises, conducts, or assists in the validation.

(12) The security coordinator and alternates of each TSA-approved validation firm under 49 CFR part 1522 subpart B and of each certified cargo screening facility.

(b) For purposes of this subpart—

Applicant means the individuals listed in paragraph (a) of this section.

Operator means an aircraft operator, foreign air carrier, and indirect air carrier listed in paragraphs (a)(1) through (a)(3) of this section, a certified cargo screening facility described in paragraph (a)(6) of this section, and a TSA-approved validator described in paragraph (a)(10) of this section.

(c) An applicant poses a security threat under this subpart when TSA determines that he or she is known to pose or is suspected of posing a threat—

(1) To national security;

(2) To transportation security; or

(3) Of terrorism.

§ 1540.203 Security threat assessment.

(a) Each operator subject to this subpart must ensure that each of the following undergoes a security threat assessment or a comparable security threat assessment described in § 1540.205:

(1) Personnel of TSA-approved validation firms, as described in § 1522.121.

(2) Cargo personnel in the United States, as described in § 1544.228.

(3) Cargo personnel in the United States, as described in § 1546.213.

(4) Individuals with unescorted access to cargo, as described in § 1548.15.

(5) Proprietors, general partners, officers, directors, and owners of an indirect air carrier, as described in § 1548.16.

(6) Personnel of certified cargo screening facilities, as described in § 1549.111.

(b) Each operator must verify the identity and work authorization of each applicant and examine the document(s) presented by the applicant to prove identity and work authorization to determine whether they appear to be genuine and relate to the applicant presenting them.

(c) Each operator must submit to TSA a security threat assessment application for each applicant that is dated and signed by the applicant and that includes the following:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other names used previously.

(2) Current mailing address, including residential address if it differs from the current mailing address; all other residential addresses for the previous five years; and e-mail address if the applicant has an e-mail address.

(3) Date and place of birth.

(4) Social security number (submission is voluntary, although failure to provide it may delay or prevent completion of the threat assessment).

(5) Gender.

(6) Country of citizenship.

(7) If the applicant is a U.S. citizen born abroad or a naturalized U.S. citizen, their U.S. passport number; or the 10-digit document number from the applicant's Certificate of Birth Abroad, Form DS–1350.

(8) If the applicant is not a U.S. citizen, the applicant's Alien Registration Number.

(9) The applicant's daytime telephone number.

(10) The applicant's current employer(s), and the address and telephone number of the employer(s).

(11) A Privacy Notice as required in the security program and the following statement:

The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact, on this application can be punished by fine or imprisonment or both (*see* section 1001 of Title 18 United States Code), and may be grounds for denial of authorization or in the case of parties regulated under this section, removal of authorization to operate under this chapter, if applicable.

I acknowledge that if I do not successfully complete the security threat assessment, the Transportation Security Administration may notify my employer. If TSA or other law enforcement agency becomes aware that I may pose an imminent threat to an operator or facility, TSA may provide limited information necessary to reduce the risk of injury or damage to the operator or facility.

(d) Each operator must retain the following for 180 days following the end of the applicant's service to the operator:

(1) The applicant's signed security threat assessment application.

(2) Copies of the applicant's document(s) used to verify identity and work authorization.

(3) Any notifications or documents sent to or received from TSA relating to the applicant's application and security threat assessment.

(4) As applicable, a copy of the applicant's credential evidencing completion of a threat assessment deemed comparable under paragraph (f) of this section.

(e) Records under this section may include electronic documents with electronic signature or other means of personal authentication, where accepted by TSA.

(f) TSA may determine that a security threat assessment conducted by another governmental agency is comparable to a security threat assessment conducted under this subpart. Individuals who have successfully completed a comparable security threat assessment are not required to undergo the security threat assessments described in this subpart. If TSA makes a comparability determination under this section, TSA will so notify the public. In making a comparability determination, TSA will consider—

(i) The minimum standards used for the security threat assessment;

(ii) The frequency of the security threat assessment;

(iii) The date of the most recent threat assessment; and

(iv) Other factors TSA deems appropriate.

(g) To apply for a comparability determination, the agency seeking the determination must contact the Assistant Program Manager, Attn: Federal Agency Comparability Check, Hazmat Threat Assessment Program, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598–6019.

(h) TSA has determined that each of the following are comparable to the security threat assessment required in this subpart:

(1) A CHRC conducted in accordance with §§ 1542.209, 1544.229, or 1544.230 that includes a name-based check conducted by TSA.

(2) A security threat assessment conducted under 49 CFR part 1572 for the Transportation Worker Identification Credential or Hazardous Materials Endorsement programs.

(3) A security threat assessment conducted for the Free and Secure Trade (FAST) program administered by U.S. Customs and Border Protection.

(i) If asserting completion of a comparable threat assessment listed in paragraph (h) of this section, an individual must—

(1) Present the credential that corresponds to successful completion of the comparable assessment to the operator so the operator may retain a copy of it; and

(2) Notify the operator when the credential that corresponds to successful completion of the comparable assessment expires or is revoked for any reason.

(j) A security threat assessment conducted under this subpart remains valid for five

years from the date that TSA issues a Determination of No Security Threat or a Final Determination of Threat Assessment, except—

(1) If the applicant is no longer authorized to be in the United States, the security threat assessment and the privileges it conveys expire on the date lawful presence expires; or

(2) If the applicant asserts completion of a comparable threat assessment, it expires five years from the date of issuance of the credential that corresponds to the comparable assessment, or the date on which the credential is revoked for any reason.

§ 1540.205 Procedures for security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA conducts under this subpart includes an intelligence-related check and a final disposition.

(b) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1540.203.

(2) Searches domestic and international government databases to determine if an applicant meets the requirements of 49 CFR 1540.201(c) or to confirm an applicant's identity.

(3) Adjudicates the results in accordance with 49 CFR 1540.201(c).

(c) *Wants, warrants, deportable aliens.* If the searches listed in paragraph (b)(2) of this section indicate that an applicant has an outstanding want or warrant, or is a deportable alien under the immigration laws of the United States, TSA sends the applicant's information to the appropriate law enforcement or immigration agency.

(d) *Final disposition.* Following completion of the procedures described in paragraph (b), the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the applicant and operator if TSA determines that the applicant meets the security threat assessment standards in 49 CFR 1540.201(c).

(2) TSA serves an Initial Determination of Threat Assessment on the applicant, if TSA determines that the applicant does not meet the security threat assessment standards in 49 CFR 1540.201(c). The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant is suspected of posing or poses a security threat;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.9; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant and the applicant's operator or other operator as approved by TSA, where appropriate, if TSA determines that the applicant does not meet the security threat assessment standards in 49 CFR 1540.201(c) and may pose an imminent threat to transportation or national security, or of terrorism. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant is suspected of posing or poses an imminent security threat;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5(h) or 1515.9(h), as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(4) If the applicant does not appeal the Initial Determination of Threat Assessment or Initial Determination of Threat Assessment and Immediate Revocation, or if TSA does not grant the appeal, TSA serves a Final Determination of Threat Assessment on the individual and the applicant.

(5) If the applicant appeals an Initial Determination of Threat Assessment, the procedures in 49 CFR 1515.5 or 1515.9 apply.

§ 1540.207 [Reserved]

§ 1540.209 Fees for security threat assessment.

This section describes the payment process for completion of the security threat assessments required under subpart.

(a) *Fees for security threat assessment.* (1) TSA routinely establishes and collects fees to conduct the security threat assessment process. These fees apply to all entities requesting a security threat assessment. TSA reviews the amount of the fee periodically, at least once every two years, to determine the current cost of conducting security threat assessments. TSA determines fee amounts and any necessary revisions to the fee amounts based on current costs, using a method of analysis consistent with widely accepted accounting principles and practices, and calculated in accordance with the

provisions of 31 U.S.C. 9701 and other applicable Federal law.

(2) TSA will publish fee amounts and any revisions to the fee amounts as a notice in the FEDERAL REGISTER.

(b) [Reserved]

(c) *Remittance of fees.* (1) The fees required under this subpart must be remitted to TSA in a form and manner acceptable to TSA each time the applicant or an aircraft operator, foreign air carrier, indirect air carrier, certified cargo screening facility, or TSA-approved validation firm submits the information required under §1540.203 or §1540.207 to TSA.

(2) Fees remitted to TSA under this subpart must be payable to the ''Transportation Security Administration'' in U.S. currency and drawn on a U.S. bank.

(3) TSA will not issue any fee refunds, unless a fee was paid in error.

Subpart D—Responsibilities of Holders of TSA–Approved Security Programs

SOURCE: 74 FR 47703, Sept. 16, 2009, unless otherwise noted.

EFFECTIVE DATE NOTE: At 74 FR 47703, Sept. 16, 2009, subpart D was added, effective Nov. 16, 2009.

§1540.301 Withdrawal of approval of a security program.

(a) *Applicability.* This section applies to holders of a security program approved or accepted by TSA under 49 CFR chapter XII, subchapter C.

(b) *Withdrawal of security program approval.* TSA may withdraw the approval of a security program, if TSA determines continued operation is contrary to security and the public interest, as follows:

(1) *Notice of proposed withdrawal of approval.* TSA will serve a Notice of Proposed Withdrawal of Approval, which notifies the holder of the security program, in writing, of the facts, charges, and applicable law, regulation, or order that form the basis of the determination.

(2) *Security program holder's reply.* The holder of the security program may respond to the Notice of Proposed Withdrawal of Approval no later than 15 calendar days after receipt of the withdrawal by providing the designated official, in writing, with any material facts, arguments, applicable law, and regulation.

(3) *TSA review.* The designated official will consider all information available, including any relevant material or information submitted by the holder of the security program, before either issuing a Withdrawal of Approval of the security program or rescinding the Notice of Proposed Withdrawal of Approval. If TSA issues a Withdrawal of Approval, it becomes effective upon receipt by the holder of the security program, or 15 calendar days after service, whichever occurs first.

(4) *Petition for reconsideration.* The holder of the security program may petition TSA to reconsider its Withdrawal of Approval by serving a petition for consideration no later than 15 calendar days after the holder of the security program receives the Withdrawal of Approval. The holder of the security program must serve the Petition for Reconsideration on the designated official. Submission of a Petition for Reconsideration will not stay the Withdrawal of Approval. The holder of the security program may request the designated official to stay the Withdrawal of Approval pending review of and decision on the Petition.

(5) *Assistant Secretary's review.* The designated official transmits the Petition together with all pertinent information to the Assistant Secretary for reconsideration. The Assistant Secretary will dispose of the Petition within 15 calendar days of receipt by either directing the designated official to rescind the Withdrawal of Approval or by affirming the Withdrawal of Approval. The decision of the Assistant Secretary constitutes a final agency order subject to judicial review in accordance with 49 U.S.C. 46110.

(6) *Emergency withdrawal.* If TSA finds that there is an emergency with respect to aviation security requiring immediate action that makes the procedures in this section contrary to the public interest, the designated official may issue an Emergency Withdrawal of Approval of a security program without first issuing a Notice of Proposed Withdrawal of Approval. The Emergency Withdrawal would be effective on the date that the holder of the security program receives the emergency withdrawal. In such a case, the designated official will send the holder of

the security program a brief statement of the facts, charges, applicable law, regulation, or order that forms the basis for the Emergency Withdrawal. The holder of the security program may submit a Petition for Reconsideration under the procedures in paragraphs (b)(4) through (b)(5) of this section; however, this petition will not stay the effective date of the Emergency Withdrawal.

(c) *Service of documents for withdrawal of approval of security program proceedings.* Service may be accomplished by personal delivery, certified mail, or express courier. Documents served on the holder of a security program will be served at its official place of business as designated in its application for approval or its security program. Documents served on TSA must be served to the address noted in the Notice of Withdrawal of Approval or Withdrawal of Approval, whichever is applicable.

(1) *Certificate of service.* An individual may attach a certificate of service to a document tendered for filing. A certificate of service must consist of a statement, dated and signed by the person filing the document, that the document was personally delivered, served by certified mail on a specific date, or served by express courier on a specific date.

(2) *Date of service.* The date of service is—

(i) The date of personal delivery;

(ii) If served by certified mail, the mailing date shown on the certificate of service, the date shown on the postmark if there is no certificate of service, or other mailing date shown by other evidence if there is no certificate of service or postmark; or

(iii) If served by express courier, the service date shown on the certificate of service, or by other evidence if there is no certificate of service.

(d) *Extension of time.* TSA may grant an extension of time to the limits set forth in this section for good cause shown. A security program holder must submit a request for an extension of time in writing, and TSA must receive it at least two days before the due date in order to be considered. TSA may grant itself an extension of time for good cause.

§ 1540.303 [Reserved]

PART 1542—AIRPORT SECURITY

Subpart A—General

Subpart B—Airport Security Program

Subpart C—Operations

Subpart D—Contingency Measures

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44913–44914, 44916–44917, 44935–44936, 44942, 46105.

SOURCE: 67 FR 8355, Feb. 22, 2002, unless otherwise noted.

Subpart A—General

§ 1542.1 Applicability of this part.

This part describes aviation security rules governing:

(a) The operation of airports regularly serving aircraft operations required to be under a security program under part 1544 of this chapter, as described in this part.

(b) The operation of airport regularly serving foreign air carrier operations required to be under a security program under part 1546 of this chapter, as described in this part.

(c) Each airport operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular issued by the Designated official for Civil Aviation Security.

(d) Each airport operator that does not have a security program under this part that serves an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter. Such airport operators must comply with §1542.5(e).

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

§1542.3 Airport security coordinator.

(a) Each airport operator must designate one or more Airport Security Coordinator(s) (ASC) in its security program.

(b) The airport operator must ensure that one or more ASCs:

(1) Serve as the airport operator's primary and immediate contact for security-related activities and communications with TSA. Any individual designated as an ASC may perform other duties in addition to those described in this paragraph (b).

(2) Is available to TSA on a 24-hour basis.

(3) Review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with this part, its security program, and applicable Security Directives.

(4) Immediately initiate corrective action for any instance of non-compliance with this part, its security program, and applicable Security Directives.

(5) Review and control the results of employment history, verification, and criminal history records checks required under §1542.209.

(6) Serve as the contact to receive notification from individuals applying for unescorted access of their intent to seek correction of their criminal history record with the FBI.

(c) After July 17, 2003, no airport operator may use, nor may it designate any person as, an ASC unless that individual has completed subject matter training, as specified in its security program, to prepare the individual to assume the duties of the position. The airport operator must maintain ASC training documentation until at least 180 days after the withdrawal of an individual's designation as an ASC.

(d) An individual's satisfactory completion of initial ASC training required under paragraph (c) of this section satisfies that requirement for all future ASC designations for that individual, except for site specific information, unless there has been a two or more year break in service as an active and designated ASC.

§1542.5 Inspection authority.

(a) Each airport operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with—

(1) This subchapter and any security program under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each airport operator must provide evidence of compliance with this part and its airport security program, including copies of records.

(c) TSA may enter and be present within secured areas, AOA's, and SIDA's without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

(d) At the request of TSA and upon the completion of SIDA training as required in a security program, each airport operator promptly must issue to TSA personnel access and identification media to provide TSA personnel with unescorted access to, and movement within, secured areas, AOA's, and SIDA's.

(e) TSA may enter and be present at an airport that does not have a security program under this part, without

access media or identification media issued or approved by an airport operator or aircraft operator, to inspect an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

Subpart B—Airport Security Program

§ 1542.101 General requirements.

(a) No person may operate an airport subject to § 1542.103 unless it adopts and carries out a security program that—

(1) Provides for the safety and security of persons and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft;

(2) Is in writing and is signed by the airport operator;

(3) Includes the applicable items listed in § 1542.103;

(4) Includes an index organized in the same subject area sequence as § 1542.103; and

(5) Has been approved by TSA.

(b) Each airport operator subject to § 1542.103 must maintain one current and complete copy of its security program and provide a copy to TSA upon request.

(c) Each airport operator subject to § 1542.103 must—

(1) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know; and

(2) Refer all requests for SSI by other persons to TSA.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

§ 1542.103 Content.

(a) *Complete program.* Except as otherwise approved by TSA, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(1) or § 1546.101(a) of this chapter, must include in its security program the following:

(1) The name, means of contact, duties, and training requirements of the ASC required under § 1542.3.

(2) [Reserved]

(3) A description of the secured areas, including—

(i) A description and map detailing boundaries and pertinent features;

(ii) Each activity or entity on, or adjacent to, a secured area that affects security;

(iii) Measures used to perform the access control functions required under § 1542.201(b)(1);

(iv) Procedures to control movement within the secured area, including identification media required under § 1542.201(b)(3); and

(v) A description of the notification signs required under § 1542.201(b)(6).

(4) A description of the AOA, including—

(i) A description and map detailing boundaries, and pertinent features;

(ii) Each activity or entity on, or adjacent to, an AOA that affects security;

(iii) Measures used to perform the access control functions required under § 1542.203(b)(1);

(iv) Measures to control movement within the AOA, including identification media as appropriate; and

(v) A description of the notification signs required under § 1542.203(b)(4).

(5) A description of the SIDA's, including—

(i) A description and map detailing boundaries and pertinent features; and

(ii) Each activity or entity on, or adjacent to, a SIDA.

(6) A description of the sterile areas, including—

(i) A diagram with dimensions detailing boundaries and pertinent features;

(ii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and

(iii) Measures used to control access as specified in § 1542.207.

(7) Procedures used to comply with § 1542.209 regarding fingerprint-based criminal history records checks.

(8) A description of the personnel identification systems as described in § 1542.211.

(9) Escort procedures in accordance with §1542.211(e).

(10) Challenge procedures in accordance with §1542.211(d).

(11) Training programs required under §§1542.213 and 1542.217(c)(2), if applicable.

(12) A description of law enforcement support used to comply with §1542.215(a).

(13) A system for maintaining the records described in §1542.221.

(14) The procedures and a description of facilities and equipment used to support TSA inspection of individuals and property, and aircraft operator or foreign air carrier screening functions of parts 1544 and 1546 of this chapter.

(15) A contingency plan required under §1542.301.

(16) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(17) Procedures for posting of public advisories as specified in §1542.305.

(18) Incident management procedures used to comply with §1542.307.

(19) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions.

(20) Each exclusive area agreement as specified in §1542.111.

(21) Each airport tenant security program as specified in §1542.113.

(b) *Supporting program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in §1544.101(a)(2) or (f), or §1546.101(b) or (c) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC, as required under §1542.3.

(2) A description of the law enforcement support used to comply with §1542.215(a).

(3) Training program for law enforcement personnel required under §1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in §1542.221.

(5) The contingency plan required under §1542.301.

(6) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(7) Procedures for public advisories as specified in §1542.305.

(8) Incident management procedures used to comply with §1542.307.

(c) *Partial program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in §1544.101(b) or §1546.101(d) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC as required under §1542.3.

(2) A description of the law enforcement support used to comply with §1542.215(b).

(3) Training program for law enforcement personnel required under §1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in §1542.221.

(5) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(6) Procedures for public advisories as specified in §1542.305.

(7) Incident management procedures used to comply with §1542.307.

(d) *Use of appendices.* The airport operator may comply with paragraphs (a), (b), and (c) of this section by including in its security program, as an appendix, any document that contains the information required by paragraphs (a), (b), and (c) of this section. The appendix must be referenced in the corresponding section(s) of the security program.

§1542.105 Approval and amendments.

(a) *Initial approval of security program.* Unless otherwise authorized by the designated official, each airport operator required to have a security program under this part must submit its initial

proposed security program to the designated official for approval at least 90 days before the date any aircraft operator or foreign air carrier required to have a security program under part 1544 or part 1546 of this chapter is expected to begin operations. Such requests will be processed as follows:

(1) The designated official, within 30 days after receiving the proposed security program, will either approve the program or give the airport operator written notice to modify the program to comply with the applicable requirements of this part.

(2) The airport operator may either submit a modified security program to the designated official for approval, or petition the Administrator to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.

(3) The designated official, upon receipt of a petition for reconsideration, either amends or withdraws the notice, or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the notice to modify, or by affirming the notice to modify.

(b) *Amendment requested by an airport operator.* Except as provided in §1542.103(c), an airport operator may submit a request to the designated official to amend its security program, as follows:

(1) The request for an amendment must be filed with the designated official at least 45 days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the designated official.

(2) Within 30 days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(3) An amendment to a security program may be approved if the designated official determines that safety and the public interest will allow it, and the proposed amendment provides the level of security required under this part.

(4) Within 30 days after receiving a denial, the airport operator may petition the Administrator to reconsider the denial.

(5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition within 30 days of receipt, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to approve the amendment or affirming the denial.

(c) *Amendment by TSA.* If safety and the public interest require an amendment, the designated official may amend a security program as follows:

(1) The designated official sends to the airport operator a notice, in writing, of the proposed amendment, fixing a period of not less than 30 days within which the airport operator may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the airport operator of any amendment adopted or rescinds the notice. If the amendment is adopted, it becomes effective not less than 30 days after the airport operator receives the notice of amendment, unless the airport operator petitions the Administrator to reconsider no later than 15 days before the effective date of the amendment. The airport operator must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice, or transmits the petition, together with any pertinent information to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the amendment, or by affirming the amendment.

(d) *Emergency amendments.* Notwithstanding paragraph (c) of this section, if the designated official finds that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air commerce that makes procedures in

this section contrary to the public interest, the designated official may issue an amendment, effective without stay on the date the airport operator receives the notice of it. In such a case, the designated official must incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The airport operator may file a petition for reconsideration under paragraph (c) of this section; however, this does not stay the effective date of the emergency amendment.

§ 1542.107 Changed conditions affecting security.

(a) After approval of the security program, each airport operator must notify TSA when changes have occurred to the—

(1) Measures, training, area descriptions, or staffing, described in the security program;

(2) Operations of an aircraft operator or foreign air carrier that would require modifications to the security program as required under § 1542.103; or

(3) Layout or physical structure of any area under the control of the airport operator, airport tenant, aircraft operator, or foreign air carrier used to support the screening process, access, presence, or movement control functions required under part 1542, 1544, or 1546 of this chapter.

(b) Each airport operator must notify TSA no more than 6 hours after the discovery of any changed condition described in paragraph (a) of this section, or within the time specified in its security program, of the discovery of any changed condition described in paragraph (a) of this section. The airport operator must inform TSA of each interim measure being taken to maintain adequate security until an appropriate amendment to the security program is approved. Each interim measure must be acceptable to TSA.

(c) For changed conditions expected to be less than 60 days duration, each airport operator must forward the information required in paragraph (b) of this section in writing to TSA within 72 hours of the original notification of the change condition(s). TSA will notify the airport operator of the disposition of the notification in writing. If approved by TSA, this written notification becomes a part of the airport security program for the duration of the changed condition(s).

(d) For changed conditions expected to be 60 days or more duration, each airport operator must forward the information required in paragraph (b) of this section in the form of a proposed amendment to the airport operator's security program, as required under § 1542.105. The request for an amendment must be made within 30 days of the discovery of the changed condition(s). TSA will respond to the request in accordance with § 1542.105.

§ 1542.109 Alternate means of compliance.

If in TSA's judgment, the overall safety and security of the airport, and aircraft operator or foreign air carrier operations are not diminished, TSA may approve a security program that provides for the use of alternate measures. Such a program may be considered only for an operator of an airport at which service by aircraft operators or foreign air carriers under part 1544 or 1546 of this chapter is determined by TSA to be seasonal or infrequent.

§ 1542.111 Exclusive area agreements.

(a) TSA may approve an amendment to an airport security program under which an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter assumes responsibility for specified security measures for all or portions of the secured area, AOA, or SIDA, including access points, as provided in § 1542.201, § 1542.203, or § 1542.205. The assumption of responsibility must be exclusive to one aircraft operator or foreign air carrier, and shared responsibility among aircraft operators or foreign air carriers is not permitted for an exclusive area.

(b) An exclusive area agreement must be in writing, signed by the airport operator and aircraft operator or foreign air carrier, and maintained in the airport security program. This agreement must contain the following:

(1) A description, a map, and, where appropriate, a diagram of the boundaries and pertinent features of each area, including individual access

points, over which the aircraft operator or foreign air carrier will exercise exclusive security responsibility.

(2) A description of the measures used by the aircraft operator or foreign air carrier to comply with § 1542.201, § 1542.203, or § 1542.205, as appropriate.

(3) Procedures by which the aircraft operator or foreign air carrier will immediately notify the airport operator and provide for alternative security measures when there are changed conditions as described in § 1542.103(a).

(c) Any exclusive area agreements in effect on November 14, 2001, must meet the requirements of this section and § 1544.227 no later than November 14, 2002.

§ 1542.113 Airport tenant security programs.

(a) TSA may approve an airport tenant security program as follows:

(1) The tenant must assume responsibility for specified security measures of the secured area, AOA, or SIDA as provided in §§ 1542.201, 1542.203, and 1542.205.

(2) The tenant may not assume responsibility for law enforcement support under § 1542.215.

(3) The tenant must assume the responsibility within the tenant's leased areas or areas designated for the tenant's exclusive use. A tenant may not assume responsibility under a tenant security program for the airport passenger terminal.

(4) Responsibility must be exclusive to one tenant, and shared responsibility among tenants is not permitted.

(5) TSA must find that the tenant is able and willing to carry out the airport tenant security program.

(b) An airport tenant security program must be in writing, signed by the airport operator and the airport tenant, and maintained in the airport security program. The airport tenant security program must include the following:

(1) A description and a map of the boundaries and pertinent features of each area over which the airport tenant will exercise security responsibilities.

(2) A description of the measures the airport tenant has assumed.

(3) Measures by which the airport operator will monitor and audit the tenant's compliance with the security program.

(4) Monetary and other penalties to which the tenant may be subject if it fails to carry out the airport tenant security program.

(5) Circumstances under which the airport operator will terminate the airport tenant security program for cause.

(6) A provision acknowledging that the tenant is subject to inspection by TSA in accordance with § 1542.5.

(7) A provision acknowledging that individuals who carry out the tenant security program are contracted to or acting for the airport operator and are required to protect sensitive information in accordance with part 1520 of this chapter, and may be subject to civil penalties for failing to protect sensitive security information.

(8) Procedures by which the tenant will immediately notify the airport operator of and provide for alternative security measures for changed conditions as described in § 1542.103(a).

(c) If TSA has approved an airport tenant security program, the airport operator may not be found to be in violation of a requirement of this part in any case in which the airport operator demonstrates that:

(1) The tenant or an employee, permittee, or invitee of the tenant, is responsible for such violation; and

(2) The airport operator has complied with all measures in its security program to ensure the tenant has complied with the airport tenant security program.

(d) TSA may amend or terminate an airport tenant security program in accordance with § 1542.105.

Subpart C—Operations

§ 1542.201 Security of the secured area.

(a) Each airport operator required to have a security program under § 1542.103(a) must establish at least one secured area.

(b) Each airport operator required to establish a secured area must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within

the secured area by doing the following:

(1) Establish and carry out measures for controlling entry to secured areas of the airport in accordance with §1542.207.

(2) Provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the secured area by an individual whose access is not authorized in accordance with its security program.

(3) Establish and carry out a personnel identification system described under §1542.211.

(4) Subject each individual to employment history verification as described in §1542.209 before authorizing unescorted access to a secured area.

(5) Train each individual before granting unescorted access to the secured area, as required in §1542.213(b).

(6) Post signs at secured area access points and on the perimeter that provide warning of the prohibition against unauthorized entry. Signs must be posted by each airport operator in accordance with its security program not later than November 14, 2003.

§1542.203 Security of the air operations area (AOA).

(a) Each airport operator required to have a security program under §1542.103(a) must establish an AOA, unless the entire area is designated as a secured area.

(b) Each airport operator required to establish an AOA must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA by doing the following:

(1) Establish and carry out measures for controlling entry to the AOA of the airport in accordance with §1542.207.

(2) Provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the AOA by an individual whose access is not authorized in accordance with its security program.

(3) Provide security information as described in §1542.213(c) to each individual with unescorted access to the AOA.

(4) Post signs on AOA access points and perimeters that provide warning of the prohibition against unauthorized entry to the AOA. Signs must be posted by each airport operator in accordance with its security program not later than November 14, 2003.

(5) If approved by TSA, the airport operator may designate all or portions of its AOA as a SIDA, or may use another personnel identification system, as part of its means of meeting the requirements of this section. If it uses another personnel identification system, the media must be clearly distinguishable from those used in the secured area and SIDA.

§1542.205 Security of the security identification display area (SIDA).

(a) Each airport operator required to have a complete program under §1542.103(a) must establish at least one SIDA, as follows:

(1) Each secured area must be a SIDA.

(2) Each part of the air operations area that is regularly used to load cargo on, or unload cargo from, an aircraft that is operated under a full program or a full all-cargo program as provided in §1544.101(a) or (h) of this chapter, or a foreign air carrier under a security program as provided in §1546.101(a), (b), or (e), must be a SIDA.

(3) Each area on an airport where cargo is present after an aircraft operator operating under a full program or a full all-cargo program under §1544.101(a) or (h) of this chapter, or a foreign air carrier operating under a security program under §1546.101(a), (b), or (e) of this chapter, or an indirect air carrier, accepts it must be a SIDA. This includes areas such as: Cargo facilities; loading and unloading vehicle docks; and areas where an aircraft operator, foreign air carrier, or indirect air carrier sorts, stores, stages, consolidates, processes, screens, or transfers cargo.

(4) Other areas of the airport may be SIDAs.

(b) Each airport operator required to establish a SIDA must establish and carry out measures to prevent the unauthorized presence and movement of individuals in the SIDA and must do the following:

(1) Establish and carry out a personnel identification system described under §1542.211.

(2) Subject each individual to a criminal history records check as described in §1542.209 before authorizing unescorted access to the SIDA.

(3) Train each individual before granting unescorted access to the SIDA, as required in §1542.213(b).

(c) An airport operator that is not required to have a complete program under §1542.103(a) is not required to establish a SIDA under this section.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

§1542.207 Access control systems.

(a) *Secured area.* Except as provided in paragraph (b) of this section, the measures for controlling entry to the secured area required under §1542.201(b)(1) must—

(1) Ensure that only those individuals authorized to have unescorted access to the secured area are able to gain entry;

(2) Ensure that an individual is immediately denied entry to a secured area when that person's access authority for that area is withdrawn; and

(3) Provide a means to differentiate between individuals authorized to have access to an entire secured area and individuals authorized access to only a particular portion of a secured area.

(b) *Alternative systems.* TSA may approve an amendment to a security program that provides alternative measures that provide an overall level of security equal to that which would be provided by the measures described in paragraph (a) of this section.

(c) *Air operations area.* The measures for controlling entry to the AOA required under §1542.203(b)(1) must incorporate accountability procedures to maintain their integrity.

(d) *Secondary access media.* An airport operator may issue a second access medium to an individual who has unescorted access to secured areas or the AOA, but is temporarily not in possession of the original access medium, if the airport operator follows measures and procedures in the security program that—

(1) Verifies the authorization of the individual to have unescorted access to secured areas or AOAs;

(2) Restricts the time period of entry with the second access medium;

(3) Retrieves the second access medium when expired;

(4) Deactivates or invalidates the original access medium until the individual returns the second access medium; and

(5) Provides that any second access media that is also used as identification media meet the criteria of §1542.211(b).

§1542.209 Fingerprint-based criminal history records checks (CHRC).

(a) *Scope.* The following persons are within the scope of this section—

(1) Each airport operator and airport user.

(2) Each individual currently having unescorted access to a SIDA, and each individual with authority to authorize others to have unescorted access to a SIDA (referred to as unescorted access authority).

(3) Each individual seeking unescorted access authority.

(4) Each airport user and aircraft operator making a certification to an airport operator pursuant to paragraph (n) of this section, or 14 CFR 108.31(n) in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001). An airport user, for the purposes of this section only, is any person other than an aircraft operator subject to §1544.229 of this chapter making a certification under this section.

(b) *Individuals seeking unescorted access authority.* Except as provided in paragraph (m) of this section, each airport operator must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based CHRC that does not disclose that he or she has a disqualifying criminal offense, as described in paragraph (d) of this section.

(c) *Individuals who have not had a CHRC.* (1) Except as provided in paragraph (m) of this section, each airport operator must ensure that after December 6, 2002, no individual retains unescorted access authority, unless the airport operator has obtained and submitted a fingerprint under this part.

(2) When a CHRC discloses a disqualifying criminal offense for which the conviction or finding of not guilty by

reason of insanity was on or after December 6, 1991, the airport operator must immediately suspend that individual's authority.

(d) *Disqualifying criminal offenses.* An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the disqualifying crimes listed in this paragraph (d) in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority. The disqualifying criminal offenses are as follows—

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.

(2) Interference with air navigation; 49 U.S.C. 46308.

(3) Improper transportation of a hazardous material; 49 U.S.C. 46312.

(4) Aircraft piracy; 49 U.S.C. 46502.

(5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504.

(6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.

(7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.

(8) Conveying false information and threats; 49 U.S.C. 46507.

(9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).

(10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.

(11) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.

(12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.

(13) Murder.

(14) Assault with intent to murder.

(15) Espionage.

(16) Sedition.

(17) Kidnapping or hostage taking.

(18) Treason.

(19) Rape or aggravated sexual abuse.

(20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.

(21) Extortion.

(22) Armed or felony unarmed robbery.

(23) Distribution of, or intent to distribute, a controlled substance.

(24) Felony arson.

(25) Felony involving a threat.

(26) Felony involving—

(i) Willful destruction of property;

(ii) Importation or manufacture of a controlled substance;

(iii) Burglary;

(iv) Theft;

(v) Dishonesty, fraud, or misrepresentation;

(vi) Possession or distribution of stolen property;

(vii) Aggravated assault;

(viii) Bribery; or

(ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

(27) Violence at international airports; 18 U.S.C. 37.

(28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d).

(e) *Fingerprint application and processing.* (1) At the time of fingerprinting, the airport operator must provide the individual to be fingerprinted a fingerprint application that includes only the following—

(i) The disqualifying criminal offenses described in paragraph (d) of this section.

(ii) A statement that the individual signing the application does not have a disqualifying criminal offense.

(iii) A statement informing the individual that Federal regulations under 49 CFR 1542.209 (l) impose a continuing obligation to disclose to the airport operator within 24 hours if he or she is convicted of any disqualifying criminal offense that occurs while he or she has unescorted access authority. After February 17, 2002, the airport operator may use statements that have already been printed referring to 14 CFR 107.209 until stocks of such statements are used up.

(iv) A statement reading, ''The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or

both. (See section 1001 of Title 18 United States Code.)''

(v) A line for the printed name of the individual.

(vi) A line for the individual's signature and date of signature.

(2) Each individual must complete and sign the application prior to submitting his or her fingerprints.

(3) The airport operator must verify the identity of the individual through two forms of identification prior to fingerprinting, and ensure that the printed name on the fingerprint application is legible. At least one of the two forms of identification must have been issued by a government authority, and at least one must include a photo.

(4) The airport operator must advise the individual that:

(i) A copy of the criminal record received from the FBI will be provided to the individual, if requested by the individual in writing; and

(ii) The ASC is the individual's point of contact if he or she has questions about the results of the CHRC.

(5) The airport operator must collect, control, and process one set of legible and classifiable fingerprints under direct observation of the airport operator or a law enforcement officer.

(6) Fingerprints may be obtained and processed electronically, or recorded on fingerprint cards approved by the FBI and distributed by TSA for that purpose.

(7) The fingerprint submission must be forwarded to TSA in the manner specified by TSA.

(f) *Fingerprinting fees.* Airport operators must pay for all fingerprints in a form and manner approved by TSA. The payment must be made at the designated rate (available from the local TSA security office) for each set of fingerprints submitted. Information about payment options is available though the designated TSA headquarters point of contact. Individual personal checks are not acceptable.

(g) *Determination of arrest status.* (1) When a CHRC on an individual seeking unescorted access authority discloses an arrest for any disqualifying criminal offense listed in paragraph (d) of this section without indicating a disposition, the airport operator must determine, after investigation, that the arrest did not result in a disqualifying offense before granting that authority. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(2) When a CHRC on an individual with unescorted access authority discloses an arrest for any disqualifying criminal offense without indicating a disposition, the airport operator must suspend the individual's unescorted access authority not later than 45 days after obtaining the CHRC unless the airport operator determines, after investigation, that the arrest did not result in a disqualifying criminal offense. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(3) The airport operator may only make the determinations required in paragraphs (g)(1) and (g)(2) of this section for individuals for whom it is issuing, or has issued, unescorted access authority, and who are not covered by a certification from an aircraft operator under paragraph (n) of this section. The airport operator may not make determinations for individuals described in §1544.229 of this chapter.

(h) *Correction of FBI records and notification of disqualification.* (1) Before making a final decision to deny unescorted access authority to an individual described in paragraph (b) of this section, the airport operator must advise him or her that the FBI criminal record discloses information that would disqualify him or her from receiving or retaining unescorted access authority and provide the individual with a copy of the FBI record if he or she requests it.

(2) The airport operator must notify an individual that a final decision has been made to grant or deny unescorted access authority.

(3) Immediately following the suspension of unescorted access authority of an individual, the airport operator must advise him or her that the FBI

criminal record discloses information that disqualifies him or her from retaining unescorted access authority and provide the individual with a copy of the FBI record if he or she requests it.

(i) *Corrective action by the individual.* The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record, subject to the following conditions—

(1) For an individual seeking unescorted access authority on or after December 6, 2001, the following applies:

(i) Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the airport operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The airport operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to granting unescorted access authority.

(ii) If no notification, as described in paragraph (h)(1) of this section, is received within 30 days, the airport operator may make a final determination to deny unescorted access authority.

(2) For an individual with unescorted access authority before December 6, 2001, the following applies: Within 30 days after being advised of suspension because the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the airport operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The airport operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to reinstating unescorted access authority.

(j) *Limits on dissemination of results.* Criminal record information provided by the FBI may be used only to carry out this section and §1544.229 of this chapter. No person may disseminate the results of a CHRC to anyone other than:

(1) The individual to whom the record pertains, or that individual's authorized representative.

(2) Officials of other airport operators who are determining whether to grant unescorted access to the individual under this part.

(3) Aircraft operators who are determining whether to grant unescorted access to the individual or authorize the individual to perform screening functions under part 1544 of this chapter.

(4) Others designated by TSA.

(k) *Recordkeeping.* The airport operator must maintain the following information:

(1) *Investigations conducted before December 6, 2001.* The airport operator must maintain and control the access or employment history investigation files, including the criminal history records results portion, or the appropriate certifications, for investigations conducted before December 6, 2001.

(2) *Fingerprint application process on or after December 6, 2001.* Except when the airport operator has received a certification under paragraph (n) of this section, the airport operator must physically maintain, control, and, as appropriate, destroy the fingerprint application and the criminal record. Only direct airport operator employees may carry out the responsibility for maintaining, controlling, and destroying criminal records.

(3) *Certification on or after December 6, 2001.* The airport operator must maintain the certifications provided under paragraph (n) of this section.

(4) *Protection of records—all investigations.* The records required by this section must be maintained in a manner that is acceptable to TSA and in a manner that protects the confidentiality of the individual.

(5) *Duration—all investigations.* The records identified in this section with regard to an individual must be maintained until 180 days after the termination of the individual's unescorted access authority. When files are no longer maintained, the criminal record must be destroyed.

(l) *Continuing responsibilities.* (1) Each individual with unescorted access authority on December 6, 2001, who had a

disqualifying criminal offense in paragraph (d) of this section on or after December 6, 1991, must, by January 7, 2002, report the conviction to the airport operator and surrender the SIDA access medium to the issuer.

(2) Each individual with unescorted access authority who has a disqualifying criminal offense must report the offense to the airport operator and surrender the SIDA access medium to the issuer within 24 hours of the conviction or the finding of not guilty by reason of insanity.

(3) If information becomes available to the airport operator or the airport user indicating that an individual with unescorted access authority has a disqualifying criminal offense, the airport operator must determine the status of the conviction. If a disqualifying offense is confirmed the airport operator must immediately revoke any unescorted access authority.

(m) *Exceptions.* Notwithstanding the requirements of this section, an airport operator must authorize the following individuals to have unescorted access authority:

(1) An employee of the Federal, state, or local government (including a law enforcement officer) who, as a condition of employment, has been subjected to an employment investigation that includes a criminal records check.

(2) Notwithstanding the requirements of this section, an airport operator may authorize the following individuals to have unescorted access authority:

(i) An individual who has been continuously employed in a position requiring unescorted access authority by another airport operator, airport user, or aircraft operator, or contractor to such an entity, provided the grant for his or her unescorted access authority was based upon a fingerprint-based CHRC through TSA or FAA.

(ii) An individual who has been continuously employed by an aircraft operator or aircraft operator contractor, in a position with authority to perform screening functions, provided the grant for his or her authority to perform screening functions was based upon a fingerprint-based CHRC through TSA or FAA.

(n) *Certifications by aircraft operators.* An airport operator is in compliance with its obligation under paragraph (b) or (c) of this section when the airport operator accepts, for each individual seeking unescorted access authority, certification from an aircraft operator subject to part 1544 of this chapter indicating it has complied with §1544.229 of this chapter for the aircraft operator's employees and contractors seeking unescorted access authority. If the airport operator accepts a certification from the aircraft operator, the airport operator may not require the aircraft operator to provide a copy of the CHRC.

(o) *Airport operator responsibility.* The airport operator must—

(1) Designate the ASC, in the security program, or a direct employee if the ASC is not a direct employee, to be responsible for maintaining, controlling, and destroying the criminal record files when their maintenance is no longer required by paragraph (k) of this section.

(2) Designate the ASC, in the security program, to serve as the contact to receive notification from individuals applying for unescorted access authority of their intent to seek correction of their FBI criminal record.

(3) Audit the employment history investigations performed by the airport operator in accordance with this section and 14 CFR 107.31 in effect prior to November 14, 2001 (see 14 CFR Parts 60 through 139 revised as of January 1, 2001), and those investigations conducted by the airport users who provided certification to the airport operator. The audit program must be set forth in the airport security program.

(p) *Airport user responsibility.* (1) The airport user must report to the airport operator information, as it becomes available, that indicates an individual with unescorted access authority may have a disqualifying criminal offense.

(2) The airport user must maintain and control, in compliance with paragraph (k) of this section, the employment history investigation files for investigations conducted before December 6, 2001, unless the airport operator decides to maintain and control the employment history investigation file.

(3) The airport user must provide the airport operator with either the name or title of the individual acting as custodian of the files described in this paragraph (p), the address of the location where the files are maintained, and the phone number of that location. The airport user must provide the airport operator and TSA with access to these files.

§ 1542.211 Identification systems.

(a) *Personnel identification system.* The personnel identification system under §§ 1542.201(b)(3) and 1542.205(b)(1) must include the following:

(1) Personnel identification media that—

(i) Convey a full-face image, full name, employer, and identification number of the individual to whom the identification medium is issued;

(ii) Indicate clearly the scope of the individual's access and movement privileges;

(iii) Indicate clearly an expiration date; and

(iv) Are of sufficient size and appearance as to be readily observable for challenge purposes.

(2) Procedures to ensure that each individual in the secured area or SIDA continuously displays the identification medium issued to that individual on the outermost garment above waist level, or is under escort.

(3) Procedures to ensure accountability through the following:

(i) Retrieving expired identification media and media of persons who no longer have unescorted access authority.

(ii) Reporting lost or stolen identification media.

(iii) Securing unissued identification media stock and supplies.

(iv) Auditing the system at a minimum of once a year or sooner, as necessary, to ensure the integrity and accountability of all identification media.

(v) As specified in the security program, revalidate the identification system or reissue identification media if a portion of all issued, unexpired identification media are lost, stolen, or otherwise unaccounted for, including identification media that are combined with access media.

(vi) Ensure that only one identification medium is issued to an individual at a time, except for personnel who are employed with more than one company and require additional identification media to carry out employment duties. A replacement identification medium may only be issued if an individual declares in writing that the medium has been lost, stolen, or destroyed.

(b) *Temporary identification media.* Each airport operator may issue personnel identification media in accordance with its security program to persons whose duties are expected to be temporary. The temporary identification media system must include procedures and methods to—

(1) Retrieve temporary identification media;

(2) Authorize the use of a temporary media for a limited time only;

(3) Ensure that temporary media are distinct from other identification media and clearly display an expiration date; and

(4) Ensure that any identification media also being used as an access media meet the criteria of § 1542.207(d).

(c) *Airport-approved identification media.* TSA may approve an amendment to the airport security program that provides for the use of identification media meeting the criteria of this section that are issued by entities other than the airport operator, as described in the security program.

(d) *Challenge program.* Each airport operator must establish and carry out a challenge program that requires each individual who has authorized unescorted access to secured areas and SIDA's to ascertain the authority of any individual who is not displaying an identification medium authorizing the individual to be present in the area. The challenge program must include procedures to challenge individuals not displaying airport approved identification media. The procedure must—

(1) Apply uniformly in secured areas, SIDAs, and exclusive areas;

(2) Describe how to challenge an individual directly or report any individual not visibly displaying an authorized identification medium, including procedures to notify the appropriate authority; and

(3) Describe support of challenge procedures, including law enforcement and any other responses to reports of individuals not displaying authorized identification media.

(e) *Escorting.* Each airport operator must establish and implement procedures for escorting individuals who do not have unescorted access authority to a secured area or SIDA that—

(1) Ensure that only individuals with unescorted access authority are permitted to escort;

(2) Ensure that the escorted individuals are continuously accompanied or monitored while within the secured area or SIDA in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted, and to take action in accordance with the airport security program;

(3) Identify what action is to be taken by the escort, or other authorized individual, should individuals under escort engage in activities other than those for which access was granted;

(4) Prescribe law enforcement support for escort procedures; and

(5) Ensure that individuals escorted into a sterile area without being screened under §1544.201 of this chapter remain under escort until they exit the sterile area, or submit to screening pursuant to §1544.201 or §1546.201 of this chapter.

(f) *Effective date.* The identification systems described in this section must be implemented by each airport operator not later than November 14, 2003.

§1542.213 Training.

(a) Each airport operator must ensure that individuals performing security-related functions for the airport operator are briefed on the provisions of this part, Security Directives, and Information Circulars, and the security program, to the extent that such individuals need to know in order to perform their duties.

(b) An airport operator may not authorize any individual unescorted access to the secured area or SIDA, except as provided in §1542.5, unless that individual has successfully completed training in accordance with TSA-approved curriculum specified in the security program. This curriculum must detail the methods of instruction, provide attendees with an opportunity to ask questions, and include at least the following topics—

(1) The unescorted access authority of the individual to enter and be present in various areas of the airport;

(2) Control, use, and display of airport-approved access and identification media;

(3) Escort and challenge procedures and the law enforcement support for these procedures;

(4) Security responsibilities as specified in §1540.105;

(5) Restrictions on divulging sensitive security information as described in part 1520 of this chapter; and

(6) Any other topics specified in the security program.

(c) An airport operator may not authorize any individual unescorted access to the AOA, except as provided in §1542.5, unless that individual has been provided information in accordance with the security program, including—

(1) The unescorted access authority of the individual to enter and be present in various areas of the airport;

(2) Control, use, and display of airport-approved access and identification media, if appropriate;

(3) Escort and challenge procedures and the law enforcement support for these procedures, where applicable;

(4) Security responsibilities as specified in §1540.105;

(5) Restrictions on divulging sensitive security information as described in part 1520 of this chapter; and

(6) Any other topics specified in the security program.

(d) Each airport operator must maintain a record of all training and information given to each individual under paragraphs (b) and (c) of this section for 180 days after the termination of that person's unescorted access authority.

(e) As to persons with unescorted access to the SIDA on November 14, 2001, training on responsibility under §1540.105 can be provided by making relevant security information available.

(f) Training described in paragraph (c) of this section must be implemented

by each airport operator not later than November 14, 2002.

§ 1542.215 Law enforcement support.

(a) In accordance with § 1542.217, each airport operator required to have a security program under § 1542.103(a) or (b) must provide:

(1) Law enforcement personnel in the number and manner adequate to support its security program.

(2) Uniformed law enforcement personnel in the number and manner adequate to support each system for screening persons and accessible property required under part 1544 or 1546 of this chapter, except to the extent that TSA provides Federal law enforcement support for the system.

(b) Each airport required to have a security program under § 1542.103(c) must ensure that:

(1) Law enforcement personnel are available and committed to respond to an incident in support of a civil aviation security program when requested by an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter.

(2) The procedures by which to request law enforcement support are provided to each aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter.

§ 1542.217 Law enforcement personnel.

(a) Each airport operator must ensure that law enforcement personnel used to meet the requirements of § 1542.215, meet the following qualifications while on duty at the airport—

(1) Have arrest authority described in paragraph (b) of this section;

(2) Are identifiable by appropriate indicia of authority;

(3) Are armed with a firearm and authorized to use it; and

(4) Have completed a training program that meets the requirements of paragraphs (c) and (d) of this section.

(b) Each airport operator must ensure that each individual used to meet the requirements of § 1542.215 have the authority to arrest, with or without a warrant, while on duty at the airport for the following violations of the criminal laws of the State and local jurisdictions in which the airport is located—

(1) A crime committed in the presence of the individual; and

(2) A felony, when the individual has reason to believe that the suspect has committed it.

(c) The training program required by paragraph (a)(4) of this section must—

(1) Meet the training standard for law enforcement officers prescribed by either the State or local jurisdiction in which the airport is located for law enforcement officers performing comparable functions.

(2) Specify and require training standards for private law enforcement personnel acceptable to TSA, if the State and local jurisdictions in which the airport is located do not prescribe training standards for private law enforcement personnel that meets the standards in paragraph (a) of this section.

(3) Include training in—

(i) The use of firearms;

(ii) The courteous and efficient treatment of persons subject to inspection, detention, search, arrest, and other aviation security activities;

(iii) The responsibilities of law enforcement personnel under the security program; and

(iv) Any other subject TSA determines is necessary.

(d) Each airport operator must document the training program required by paragraph (a)(4) of this section and maintain documentation of training at a location specified in the security program until 180 days after the departure or removal of each person providing law enforcement support at the airport.

§ 1542.219 Supplementing law enforcement personnel.

(a) When TSA decides, after being notified by an airport operator as prescribed in this section, that not enough qualified State, local, and private law enforcement personnel are available to carry out the requirements of § 1542.215, TSA may authorize the airport operator to use, on a reimbursable basis, personnel employed by TSA, or by another department, agency, or instrumentality of the Government with the consent of the head of the department,

agency, or instrumentality to supplement State, local, and private law enforcement personnel.

(b) Each request for the use of Federal personnel must be submitted to TSA and include the following information:

(1) The number of passengers enplaned at the airport during the preceding calendar year and the current calendar year as of the date of the request.

(2) The anticipated risk of criminal violence, sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

(3) A copy of that portion of the security program which describes the law enforcement support necessary to comply with § 1542.215.

(4) The availability of law enforcement personnel who meet the requirements of § 1542.217, including a description of the airport operator's efforts to obtain law enforcement support from State, local, and private agencies and the responses of those agencies.

(5) The airport operator's estimate of the number of Federal personnel needed to supplement available law enforcement personnel and the period of time for which they are needed.

(6) A statement acknowledging responsibility for providing reimbursement for the cost of providing Federal personnel.

(7) Any other information TSA considers necessary.

(c) In response to a request submitted in accordance with this section, TSA may authorize, on a reimbursable basis, the use of personnel employed by a Federal agency, with the consent of the head of that agency.

§ 1542.221 Records of law enforcement response.

(a) Each airport operator must ensure that—

(1) A record is made of each law enforcement action taken in furtherance of this part; and

(2) The record is maintained for a minimum of 180 days.

(b) Data developed in response to paragraph (a) of this section must include at least the following, except as authorized by TSA:

(1) The number and type of weapons, explosives, or incendiaries discovered during any passenger-screening process, and the method of detection of each.

(2) The number of acts and attempted acts of aircraft piracy.

(3) The number of bomb threats received, real and simulated bombs found, and actual detonations on the airport.

(4) The number of arrests, including—

(i) Name, address, and the immediate disposition of each individual arrested;

(ii) Type of weapon, explosive, or incendiary confiscated, as appropriate; and

(iii) Identification of the aircraft operators or foreign air carriers on which the individual arrested was, or was scheduled to be, a passenger or which screened that individual, as appropriate.

Subpart D—Contingency Measures

§ 1542.301 Contingency plan.

(a) Each airport operator required to have a security program under § 1542.103(a) and (b) must adopt a contingency plan and must:

(1) Implement its contingency plan when directed by TSA.

(2) Conduct reviews and exercises of its contingency plan as specified in the security program with all persons having responsibilities under the plan.

(3) Ensure that all parties involved know their responsibilities and that all information contained in the plan is current.

(b) TSA may approve alternative implementation measures, reviews, and exercises to the contingency plan which will provide an overall level of security equal to the contingency plan under paragraph (a) of this section.

§ 1542.303 Security Directives and Information Circulars.

(a) TSA may issue an Information Circular to notify airport operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA

issues a Security Directive setting forth mandatory measures.

(b) Each airport operator must comply with each Security Directive issued to the airport operator within the time prescribed in the Security Directive.

(c) Each airport operator that receives a Security Directive must—

(1) Within the time prescribed in the Security Directive, verbally acknowledge receipt of the Security Directive to TSA.

(2) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(d) In the event that the airport operator is unable to implement the measures in the Security Directive, the airport operator must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval. The airport operator must submit the proposed alternative measures within the time prescribed in the Security Directive. The airport operator must implement any alternative measures approved by TSA.

(e) Each airport operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.

(f) Each airport operator that receives a Security Directive or an Information Circular and each person who receives information from a Security Directive or an Information Circular must:

(1) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need-to-know.

(2) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those who have an operational need to know without the prior written consent of TSA.

§ 1542.305 Public advisories.

When advised by TSA, each airport operator must prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures. This information must be posted in the manner specified in the security program and for such a period of time determined by the Secretary of Transportation.

§ 1542.307 Incident management.

(a) Each airport operator must establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

(b) Immediately upon direct or referred receipt of a threat of any of the incidents described in paragraph (a) of this section, each airport operator must—

(1) Evaluate the threat in accordance with its security program;

(2) Initiate appropriate action as specified in the Airport Emergency Plan under 14 CFR 139.325; and

(3) Immediately notify TSA of acts, or suspected acts, of unlawful interference to civil aviation operations, including specific bomb threats to aircraft and airport facilities.

(c) Airport operators required to have a security program under §1542.103(c) but not subject to 14 CFR part 139, must develop emergency response procedures to incidents of threats identified in paragraph (a) of this section.

(d) To ensure that all parties know their responsibilities and that all procedures are current, at least once every 12 calendar months each airport operator must review the procedures required in paragraphs (a) and (b) of this section with all persons having responsibilities for such procedures.

PART 1544—AIRCRAFT OPERATOR SECURITY: AIR CARRIERS AND COMMERCIAL OPERATORS

Subpart A—General

Sec.

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44913–44914, 44916–44918, 44932, 44935–44936, 44942, 46105.

SOURCE: 67 FR 8364, Feb. 22, 2002, unless otherwise noted.

Subpart A—General

§ 1544.1 Applicability of this part.

(a) This part prescribes aviation security rules governing the following:

(1) The operations of aircraft operators holding operating certificates under 14 CFR part 119 for scheduled passenger operations, public charter passenger operations, private charter passenger operations; the operations of aircraft operators holding operating certificates under 14 CFR part 119 operating aircraft with a maximum certificated takeoff weight of 12,500 pounds or more; and other aircraft operators adopting and obtaining approval of an aircraft operator security program.

(2) Each law enforcement officer flying armed aboard an aircraft operated by an aircraft operator described in paragraph (a)(1) of this section.

(3) Each aircraft operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular issued by TSA.

(b) As used in this part, ''aircraft operator'' means an aircraft operator subject to this part as described in §1544.101.

[67 FR 8364, Feb. 22, 2002, as amended at 67 FR 8209, Feb. 22, 2002]

§ 1544.3 TSA inspection authority.

(a) Each aircraft operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with—

(1) This subchapter and any security program under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each aircraft operator must provide evidence of compliance with this part and its security program, including copies of records.

(c) TSA may enter and be present within secured areas, AOAs, SIDAs, and other areas where security measures required by TSA are carried out, without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

(d) At the request of TSA and the completion of SIDA training as required in a security program, each aircraft operator must promptly issue to TSA personnel access and identification media to provide TSA personnel with unescorted access to, and movement within, areas controlled by the aircraft operator under an exclusive area agreement.

[67 FR 8364, Feb. 22, 2002, as amended at 71 FR 30510, May 26, 2006]

Subpart B—Security Program

§ 1544.101 Adoption and implementation.

(a) *Full program.* Each aircraft operator must carry out subparts C, D, and E of this part and must adopt and carry out a security program that meets the requirements of § 1544.103 for each of the following operations:

(1) A scheduled passenger or public charter passenger operation with an aircraft having a passenger seating configuration of 61 or more seats.

(2) A scheduled passenger or public charter passenger operation with an aircraft having a passenger seating configuration of 60 or fewer seats when passengers are enplaned from or deplaned into a sterile area.

(b) *Partial program—adoption.* Each aircraft operator must carry out the requirements specified in paragraph (c) of this section for each of the following operations:

(1) A scheduled passenger or public charter passenger operation with an aircraft having a passenger-seating configuration of 31 or more but 60 or fewer seats that does not enplane from or deplane into a sterile area.

(2) A scheduled passenger or public charter passenger operation with an aircraft having a passenger-seating configuration of 60 or fewer seats engaged in operations to, from, or outside the United States that does not enplane from or deplane into a sterile area.

(c) *Partial program-content:* For operations described in paragraph (b) of this section, the aircraft operator must carry out the following, and must adopt and carry out a security program that meets the applicable requirements in § 1544.103 (c):

(1) The requirements of §§ 1544.215, 1544.217, 1544.219, 1544.223, 1544.230, 1544.235, 1544.237, 1544.301, 1544.303, and 1544.305.

(2) Other provisions of subparts C, D, and E of this part that TSA has approved upon request.

(3) The remaining requirements of subparts C, D, and E when TSA notifies the aircraft operator in writing that a security threat exists concerning that operation.

(d) *Twelve-five program-adoption:* Each aircraft operator must carry out the requirements of paragraph (e) of this section for each operation that meets all of the following—

(1) Is an aircraft with a maximum certificated takeoff weight of more than 12,500 pounds;

(2) Is in scheduled or charter service;

(3) Is carrying passengers or cargo or both; and

(4) Is not under a full program, partial program, or full all-cargo program under paragraph (a), (b), or (h) of this section.

(e) *Twelve-five program-contents:* For each operation described in paragraph (d) of this section, the aircraft operator must carry out the following, and must adopt and carry out a security program that meets the applicable requirements of § 1544.103 (c):

(1) The requirements of §§ 1544.215, 1544.217, 1544.219, 1544.223, 1544.230, 1544.235, 1544.237, 1544.301(a) and (b), 1544.303, and 1544.305; and in addition, for all-cargo operations of §§ 1544.202, 1544.205(a), (b), (d), and (f).

(2) Other provisions of subparts C, D, and E that TSA has approved upon request.

(3) The remaining requirements of subparts C, D, and E when TSA notifies the aircraft operator in writing that a security threat exists concerning that operation.

(f) *Private charter program.* In addition to paragraph (d) of this section, if applicable, each aircraft operator must carry out §§ 1544.201, 1544.207, 1544.209, 1544.211, 1544.215, 1544.217, 1544.219, 1544.225, 1544.229, 1544.230, 1544.233, 1544.235, 1544.303, and 1544.305, and subpart E of this part and—

(1) Must adopt and carry out a security program that meets the applicable requirements of § 1544.103 for each private charter passenger operation in which—

(i) The passengers are enplaned from or deplaned into a sterile area; or

(ii) The aircraft has a maximum certificated takeoff weight greater than 45,500 kg (100,309.3 pounds), or a passenger-seating configuration of 61 or more, and is not a government charter under paragraph (2) of the definition of private charter in § 1540.5 of this chapter.

(2) The Administrator may authorize alternate procedures under paragraph (f)(1) of this section as appropriate.

(g) *Limited program:* In addition to paragraph (d) of this section, if applicable, TSA may approve a security program after receiving a request by an aircraft operator holding a certificate under 14 CFR part 119, other than one identified in paragraph (a), (b), (d), or (f) of this section. The aircraft operator must—

(1) Carry out selected provisions of subparts C, D, and E;

(2) Carry out the provisions of § 1544.305, as specified in its security program; and

(3) Adopt and carry out a security program that meets the applicable requirements of § 1544.103 (c).

(h) *Full all-cargo program—adoption:* Each aircraft operator must carry out the requirements of paragraph (i) of this section for each operation that is—

(1) In an aircraft with a maximum certificated takeoff weight of more than 45,500 kg (100,309.3 pounds); and

(2) Carrying cargo and authorized persons and no passengers.

(i) *Full all-cargo program—contents:* For each operation described in paragraph (h) of this section, the aircraft operator must carry out the following, and must adopt and carry out a security program that meets the applicable requirements of § 1544.103(c):

(1) The requirements of §§ 1544.202, 1544.205, 1544.207, 1544.209, 1544.211, 1544.215, 1544.217, 1544.219, 1544.225, 1544.227, 1544.228, 1544.229, 1544.230, 1544.231, 1544.233, 1544.235, 1544.237, 1544.301, 1544.303, and 1544.305.

(2) Other provisions of subpart C of this part that TSA has approved upon request.

(3) The remaining requirements of subpart C of this part when TSA notifies the aircraft operator in writing that a security threat exists concerning that operation.

[67 FR 8364, Feb. 22, 2002, as amended at 67 FR 8209, Feb. 22, 2002; 67 FR 41639, June 19, 2002; 67 FR 79887, Dec. 31, 2002; 71 FR 30510, May 26, 2006]

§ 1544.103 Form, content, and availability.

(a) *General requirements.* Each security program must:

(1) Provide for the safety of persons and property traveling on flights provided by the aircraft operator against acts of criminal violence and air piracy, and the introduction of explosives, incendiaries, or weapons aboard an aircraft.

(2) Be in writing and signed by the aircraft operator or any person delegated authority in this matter.

(3) Be approved by TSA.

(b) *Availability.* Each aircraft operator having a security program must:

(1) Maintain an original copy of the security program at its corporate office.

(2) Have accessible a complete copy, or the pertinent portions of its security program, or appropriate implementing instructions, at each airport served. An electronic version of the program is adequate.

(3) Make a copy of the security program available for inspection upon request of TSA.

(4) Restrict the distribution, disclosure, and availability of information contained in the security program to

persons with a need-to-know as described in part 1520 of this chapter.

(5) Refer requests for such information by other persons to TSA.

(c) *Content.* The security program must include, as specified for that aircraft operator in §1544.101, the following:

(1) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.201 regarding the acceptance and screening of individuals and their accessible property, including, if applicable, the carriage weapons as part of State-required emergency equipment.

(2) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.203 regarding the acceptance and screening of checked baggage.

(3) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.205 regarding the acceptance and screening of cargo.

(4) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.207 regarding the screening of individuals and property.

(5) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.209 regarding the use of metal detection devices.

(6) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.211 regarding the use of x-ray systems.

(7) The procedures and description of the facilities and equipment used to comply with the requirements of §1544.213 regarding the use of explosives detection systems.

(8) The procedures used to comply with the requirements of §1544.215 regarding the responsibilities of security coordinators. The names of the Aircraft Operator Security Coordinator (AOSC) and any alternate, and the means for contacting the AOSC(s) on a 24-hour basis, as provided in §1544.215.

(9) The procedures used to comply with the requirements of §1544.217 regarding the requirements for law enforcement personnel.

(10) The procedures used to comply with the requirements of §1544.219 regarding carriage of accessible weapons.

(11) The procedures used to comply with the requirements of §1544.221 regarding carriage of prisoners under the control of armed law enforcement officers.

(12) The procedures used to comply with the requirements of §1544.223 regarding transportation of Federal Air Marshals.

(13) The procedures and description of the facilities and equipment used to perform the aircraft and facilities control function specified in §1544.225.

(14) The specific locations where the air carrier has entered into an exclusive area agreement under §1544.227.

(15) The procedures used to comply with the applicable requirements of §§1544.229 and 1544.230 regarding fingerprint-based criminal history records checks.

(16) The procedures used to comply with the requirements of §1544.231 regarding personnel identification systems.

(17) The procedures and syllabi used to accomplish the training required under §1544.233.

(18) The procedures and syllabi used to accomplish the training required under §1544.235.

(19) An aviation security contingency plan as specified under §1544.301.

(20) The procedures used to comply with the requirements of §1544.303 regarding bomb and air piracy threats.

(21) The procedures used to comply with §1544.237 regarding flight deck privileges.

(22) The Aircraft Operator Implementation Plan (AOIP) as required under 49 CFR 1560.109.

[67 FR 8364, Feb. 22, 2002, as amended at 67 FR 8209, Feb. 22, 2002; 73 FR 64061, Oct. 28, 2008]

§1544.105 Approval and amendments.

(a) *Initial approval of security program.* Unless otherwise authorized by TSA, each aircraft operator required to have a security program under this part must submit its proposed security program to the designated official for approval at least 90 days before the intended date of passenger operations. The proposed security program must

meet the requirements applicable to its operation as described in §1544.101. Such requests will be processed as follows:

(1) The designated official, within 30 days after receiving the proposed aircraft operator security program, will either approve the program or give the aircraft operator written notice to modify the program to comply with the applicable requirements of this part.

(2) The aircraft operator may either submit a modified security program to the designated official for approval, or petition the Administrator to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.

(3) The designated official, upon receipt of a petition for reconsideration, either amends or withdraws the notice, or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the notice to modify, or by affirming the notice to modify.

(b) *Amendment requested by an aircraft operator.* An aircraft operator may submit a request to TSA to amend its security program as follows:

(1) The request for an amendment must be filed with the designated official at least 45 days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the designated official.

(2) Within 30 days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(3) An amendment to an aircraft operator security program may be approved if the designated official determines that safety and the public interest will allow it, and the proposed amendment provides the level of security required under this part.

(4) Within 30 days after receiving a denial, the aircraft operator may petition the Administrator to reconsider the denial. A petition for reconsideration must be filed with the designated official.

(5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to approve the amendment, or affirming the denial.

(6) Any aircraft operator may submit a group proposal for an amendment that is on behalf of it and other aircraft operators that co-sign the proposal.

(c) *Amendment by TSA.* If safety and the public interest require an amendment, TSA may amend a security program as follows:

(1) The designated official notifies the aircraft operator, in writing, of the proposed amendment, fixing a period of not less than 30 days within which the aircraft operator may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the aircraft operator of any amendment adopted or rescinds the notice. If the amendment is adopted, it becomes effective not less than 30 days after the aircraft operator receives the notice of amendment, unless the aircraft operator petitions the Administrator to reconsider no later than 15 days before the effective date of the amendment. The aircraft operator must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the amendment, or by affirming the amendment.

(d) *Emergency amendments.* If the designated official finds that there is an emergency requiring immediate action with respect to safety in air transportation or in air commerce that makes procedures in this section contrary to

the public interest, the designated official may issue an amendment, without the prior notice and comment procedures in paragraph (c) of this section, effective without stay on the date the aircraft operator receives notice of it. In such a case, the designated official will incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The aircraft operator may file a petition for reconsideration under paragraph (c) of this section; however, this does not stay the effective date of the emergency amendment.

Subpart C—Operations

§ 1544.201 Acceptance and screening of individuals and accessible property.

(a) *Preventing or deterring the carriage of any explosive, incendiary, or deadly or dangerous weapon.* Each aircraft operator must use the measures in its security program to prevent or deter the carriage of any weapon, explosive, or incendiary on or about each individual's person or accessible property before boarding an aircraft or entering a sterile area.

(b) *Screening of individuals and accessible property.* Except as provided in its security program, each aircraft operator must ensure that each individual entering a sterile area at each preboard screening checkpoint for which it is responsible, and all accessible property under that individual's control, are inspected for weapons, explosives, and incendiaries as provided in § 1544.207.

(c) *Refusal to transport.* Each aircraft operator must deny entry into a sterile area and must refuse to transport—

(1) Any individual who does not consent to a search or inspection of his or her person in accordance with the system prescribed in this part; and

(2) Any property of any individual or other person who does not consent to a search or inspection of that property in accordance with the system prescribed by this part.

(d) *Prohibitions on carrying a weapon, explosive, or incendiary.* Except as provided in §§ 1544.219, 1544.221, and 1544.223, no aircraft operator may permit any individual to have a weapon, explosive, or incendiary, on or about the individual's person or accessible property when onboard an aircraft.

(e) *Staffing.* Each aircraft operator must staff its security screening checkpoints with supervisory and non-supervisory personnel in accordance with the standards specified in its security program.

§ 1544.202 Persons and property onboard an all-cargo aircraft.

Each aircraft operator operating under a full all-cargo program, or a twelve-five program in an all-cargo operation, must apply the security measures in its security program for persons who board the aircraft for transportation, and for their property, to prevent or deter the carriage of any unauthorized persons, and any unauthorized weapons, explosives, incendiaries, and other destructive devices, items, or substances.

[71 FR 30510, May 26, 2006]

§ 1544.203 Acceptance and screening of checked baggage.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each aircraft operator must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized explosive or incendiary onboard aircraft in checked baggage.

(b) *Acceptance.* Each aircraft operator must ensure that checked baggage carried in the aircraft is received by its authorized aircraft operator representative.

(c) *Screening of checked baggage.* Except as provided in its security program, each aircraft operator must ensure that all checked baggage is inspected for explosives and incendiaries before loading it on its aircraft, in accordance with § 1544.207.

(d) *Control.* Each aircraft operator must use the procedures in its security program to control checked baggage that it accepts for transport on an aircraft, in a manner that:

(1) Prevents the unauthorized carriage of any explosive or incendiary aboard the aircraft.

(2) Prevents access by persons other than an aircraft operator employee or its agent.

(e) *Refusal to transport.* Each aircraft operator must refuse to transport any individual's checked baggage or property if the individual does not consent to a search or inspection of that checked baggage or property in accordance with the system prescribed by this part.

(f) *Firearms in checked baggage.* No aircraft operator may knowingly permit any person to transport in checked baggage:

(1) Any loaded firearm(s).

(2) Any unloaded firearm(s) unless—

(i) The passenger declares to the aircraft operator, either orally or in writing before checking the baggage that any firearm carried in the baggage is unloaded;

(ii) The firearm is carried in a hard-sided container;

(iii) The container in which it is carried is locked, and only the individual checking the baggage retains the key or combination; and

(iv) The checked baggage containing the firearm is carried in an area that is inaccessible to passengers, and is not carried in the flightcrew compartment,.

(3) Any unauthorized explosive or incendiary.

(g) *Ammunition.* This section does not prohibit the carriage of ammunition in checked baggage or in the same container as a firearm. Title 49 CFR part 175 provides additional requirements governing carriage of ammunition on aircraft.

§ 1544.205 Acceptance and screening of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each aircraft operator operating under a full program, a full all-cargo program, or a twelve-five program in an all-cargo operation, must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized persons, and any unauthorized explosives, incendiaries, and other destructive substances or items in cargo onboard an aircraft.

(b) *Screening and inspection of cargo.* Each aircraft operator operating under a full program or a full all-cargo program, or a twelve-five program in an all-cargo operation, must ensure that cargo is screened and inspected for any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item as provided in the aircraft operator's security program and §1544.207, and as provided in §1544.239 for operations under a full program, before loading it on its aircraft.

(c) *Control.* Each aircraft operator operating under a full program or a full all-cargo program must use the procedures in its security program to control cargo that it accepts for transport on an aircraft in a manner that:

(1) Prevents the carriage of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item in cargo onboard an aircraft.

(2) Prevents unescorted access by persons other than an authorized aircraft operator employee or agent, or persons authorized by the airport operator or host government.

(d) *Refusal to transport.* Except as otherwise provided in its program, each aircraft operator operating under a full program, a full all-cargo program, or a twelve-five program in an all-cargo operation, must refuse to transport any cargo if the shipper does not consent to a search or inspection of that cargo in accordance with the system prescribed by this part.

(e) *Acceptance of cargo only from specified persons.* Each aircraft operator operating under a full program or a full all-cargo program may accept cargo for air transportation only from the shipper, or from an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program, as provided in its security program.

(f) *Acceptance and screening of cargo outside the United States.* For cargo to be loaded on its aircraft outside the United States, each aircraft operator must carry out the requirements of its security program.

[71 FR 30510, May 26, 2006]

EFFECTIVE DATE NOTE: At 74 FR 47703, Sept. 16, 2009, §1544.205 was amended by revising paragraph (e) and adding a new paragraph (g), effective November 16, 2009. For

the convenience of the user, the added and revised text is set forth as follows:

§ 1544.205 Acceptance and screening of cargo.

* * * * *

(e) *Acceptance of cargo only from specified persons.* Each aircraft operator operating under a full program or a full all-cargo program may accept cargo to be loaded in the United States for air transportation only from the shipper, an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program, or, in the case of an operator under a full program, from a certified cargo screening facility, as provided in its security program.

* * * * *

(g) *Screening of cargo loaded inside the United States by a full program operator.* For cargo to be loaded in the United States, each operator under a full program in §1544.101(a) must ensure that all cargo is screened in the United States as follows:

(1) *Amount screened.* (i) Not later than February 3, 2009, each operator under a full program must ensure that at least 50 percent of its cargo is screened prior to transport on a passenger aircraft.

(ii) Not later than August 3, 2010, each operator under a full program must ensure that 100 percent of its cargo is screened prior to transport on a passenger aircraft.

(2) *Methods of screening.* For the purposes of this paragraph (g), the aircraft operator must ensure that cargo is screened using a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security, as provided in its security program. Such methods may include TSA-approved x-ray systems, explosives detection systems, explosives trace detection, explosives detection canine teams certified by TSA, or a physical search together with manifest verification, or other method approved by TSA.

(3) *Limitation on who may conduct screening.* Screening must be conducted by the aircraft operator on an airport with a complete program under 49 CFR part 1542, by another aircraft operator or foreign air carrier operating under a security program under this chapter with a comparable cargo security program on an airport, by a certified cargo screening facility in accordance with 49 CFR part 1549, or by TSA. If an aircraft operator or foreign air carrier screens cargo off an airport, it must do so as a certified cargo screening facility in accordance with part 1549.

(4) *Verification.* The aircraft operator must verify that the chain of custody measures for the screened cargo are intact prior to loading such cargo on aircraft, or must ensure that the cargo is re-screened in accordance with this chapter.

§ 1544.207 Screening of individuals and property.

(a) *Applicability of this section.* This section applies to the inspection of individuals, accessible property, checked baggage, and cargo as required under this part.

(b) *Locations within the United States at which TSA conducts screening.* Each aircraft operator must ensure that the individuals or property have been inspected by TSA before boarding or loading on its aircraft. This paragraph applies when TSA is conducting screening using TSA employees or when using companies under contract with TSA.

(c) *Aircraft operator conducting screening.* Each aircraft operator must use the measures in its security program and in subpart E of this part to inspect the individual or property. This paragraph does not apply at locations identified in paragraphs (b) and (d) of this section.

(d) *Locations outside the United States at which the foreign government conducts screening.* Each aircraft operator must ensure that all individuals and property have been inspected by the foreign government. This paragraph applies when the host government is conducting screening using government employees or when using companies under contract with the government.

§ 1544.209 Use of metal detection devices.

(a) No aircraft operator may use a metal detection device within the United States or under the aircraft operator's operational control outside the United States to inspect persons, unless specifically authorized under a security program under this part. No aircraft operator may use such a device contrary to its security program.

(b) Metal detection devices must meet the calibration standards established by TSA.

§ 1544.211 Use of X-ray systems.

(a) *TSA authorization required.* No aircraft operator may use any X-ray system within the United States or under the aircraft operator's operational control outside the United States to inspect accessible property or checked baggage, unless specifically authorized under its security program. No aircraft operator may use such a system in a manner contrary to its security program. TSA authorizes aircraft operators to use X-ray systems for inspecting accessible property or checked baggage under a security program if the aircraft operator shows that—

(1) The system meets the standards for cabinet X-ray systems primarily for the inspection of baggage issued by the Food and Drug Administration (FDA) and published in 21 CFR 1020.40;

(2) A program for initial and recurrent training of operators of the system is established, which includes training in radiation safety, the efficient use of X-ray systems, and the identification of weapons, explosives, and incendiaries; and

(3) The system meets the imaging requirements set forth in its security program using the step wedge specified in American Society for Testing Materials (ASTM) Standard F792–88 (Reapproved 1993). This standard is incorporated by reference in paragraph (g) of this section.

(b) *Annual radiation survey.* No aircraft operator may use any X-ray system unless, within the preceding 12 calendar months, a radiation survey is conducted that shows that the system meets the applicable performance standards in 21 CFR 1020.40.

(c) *Radiation survey after installation or moving.* No aircraft operator may use any X-ray system after the system has been installed at a screening point or after the system has been moved unless a radiation survey is conducted which shows that the system meets the applicable performance standards in 21 CFR 1020.40. A radiation survey is not required for an X-ray system that is designed and constructed as a mobile unit and the aircraft operator shows that it can be moved without altering its performance.

(d) *Defect notice or modification order.* No aircraft operator may use any X-ray system that is not in full compliance with any defect notice or modification order issued for that system by the FDA, unless the FDA has advised TSA that the defect or failure to comply does not create a significant risk of injury, including genetic injury, to any person.

(e) *Signs and inspection of photographic equipment and film.* (1) At locations at which an aircraft operator uses an X-ray system to inspect accessible property the aircraft operator must ensure that a sign is posted in a conspicuous place at the screening checkpoint. At locations outside the United States at which a foreign government uses an X-ray system to inspect accessible property the aircraft operator must ensure that a sign is posted in a conspicuous place at the screening checkpoint.

(2) At locations at which an aircraft operator or TSA uses an X-ray system to inspect checked baggage the aircraft operator must ensure that a sign is posted in a conspicuous place where the aircraft operator accepts checked baggage.

(3) The signs required under this paragraph (e) must notify individuals that such items are being inspected by an X-ray and advise them to remove all X-ray, scientific, and high-speed film from accessible property and checked baggage before inspection. This sign must also advise individuals that they may request that an inspection be made of their photographic equipment and film packages without exposure to an X-ray system. If the X-ray system exposes any accessible property or checked baggage to more than one milliroentgen during the inspection, the sign must advise individuals to remove film of all kinds from their articles before inspection.

(4) If requested by individuals, their photographic equipment and film packages must be inspected without exposure to an X-ray system.

(f) *Radiation survey verification after installation or moving.* Each aircraft operator must maintain at least one copy of the results of the most recent radiation survey conducted under paragraph (b) or (c) of this section and must make it available for inspection upon

request by TSA at each of the following locations—

(1) The aircraft operator's principal business office; and

(2) The place where the X-ray system is in operation.

(g) *Incorporation by reference.* The American Society for Testing and Materials (ASTM) Standard F792–88 (Reapproved 1993), ''Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas,'' is approved for incorporation by reference by the Director of the Federal Register pursuant to 5 U.S.C. 552(a) and 1 CFR part 51. ASTM Standard F792–88 may be examined at the Department of Transportation (DOT) Docket, 400 Seventh Street SW, Room Plaza 401, Washington, DC 20590, or on DOT's Docket Management System (DMS) web page at *http://dms.dot.gov/search* (under docket number FAA–2001–8725). Copies of the standard may be examined also at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741–6030, or go to: *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html*. In addition, ASTM Standard F792–88 (Reapproved 1993) may be obtained from the American Society for Testing and Materials, 100 Barr Harbor Drive, West Conshohocken, PA 19428–2959.

(h) *Duty time limitations.* Each aircraft operator must comply with the X-ray operator duty time limitations specified in its security program.

[67 FR 8364, Feb. 22, 2002, as amended at 69 FR 18803, Apr. 9, 2004]

§ 1544.213 Use of explosives detection systems.

(a) *Use of explosive detection equipment.* If TSA so requires by an amendment to an aircraft operator's security program, each aircraft operator required to conduct screening under a security program must use an explosives detection system approved by TSA to screen checked baggage on international flights.

(b) *Signs and inspection of photographic equipment and film.* (1) At locations at which an aircraft operator or TSA uses an explosives detection system that uses X-ray technology to inspect checked baggage the aircraft operator must ensure that a sign is posted in a conspicuous place where the aircraft operator accepts checked baggage. The sign must notify individuals that such items are being inspected by an explosives detection system and advise them to remove all X-ray, scientific, and high-speed film from checked baggage before inspection. This sign must also advise individuals that they may request that an inspection be made of their photographic equipment and film packages without exposure to an explosives detection system.

(2) If the explosives detection system exposes any checked baggage to more than one milliroentgen during the inspection the aircraft operator must post a sign which advises individuals to remove film of all kinds from their articles before inspection. If requested by individuals, their photographic equipment and film packages must be inspected without exposure to an explosives detection system.

§ 1544.215 Security coordinators.

(a) *Aircraft Operator Security Coordinator.* Each aircraft operator must designate and use an Aircraft Operator Security Coordinator (AOSC). The AOSC and any alternates must be appointed at the corporate level and must serve as the aircraft operator's primary contact for security-related activities and communications with TSA, as set forth in the security program. Either the AOSC, or an alternate AOSC, must be available on a 24-hour basis.

(b) *Ground Security Coordinator.* Each aircraft operator must designate and use a Ground Security Coordinator for each domestic and international flight departure to carry out the Ground Security Coordinator duties specified in the aircraft operator's security program. The Ground Security Coordinator at each airport must conduct the following daily:

(1) A review of all security-related functions for which the aircraft operator is responsible, for effectiveness and compliance with this part, the aircraft operator's security program, and applicable Security Directives.

(2) Immediate initiation of corrective action for each instance of noncompliance with this part, the aircraft operator's security program, and applicable Security Directives. At foreign airports where such security measures are provided by an agency or contractor of a host government, the aircraft operator must notify TSA for assistance in resolving noncompliance issues.

(c) *In-flight Security Coordinator.* Each aircraft operator must designate and use the pilot in command as the In-flight Security Coordinator for each domestic and international flight to perform duties specified in the aircraft operator's security program.

§ 1544.217 Law enforcement personnel.

(a) The following applies to operations at airports within the United States that are not required to hold a security program under part 1542 of this chapter.

(1) For operations described in § 1544.101(a) each aircraft operator must provide for law enforcement personnel meeting the qualifications and standards specified in §§ 1542.215 and 1542.217 of this chapter.

(2) For operations under a partial program under § 1544.101(b) and (c), a twelve-five program under § 1544.101(d) and (e), a private charter program under § 1544.101(f), or a full all-cargo program under § 1544.101(h) and (i), each aircraft operator must—

(i) Arrange for law enforcement personnel meeting the qualifications and standards specified in § 1542.217 of this chapter to be available to respond to an incident; and

(ii) Provide its employees, including crewmembers, current information regarding procedures for obtaining law enforcement assistance at that airport.

(b) The following applies to operations at airports required to hold security programs under part 1542 of this chapter. For operations under a partial program under § 1544.101(b) and (c), a twelve-five program under § 1544.101(d) and (e), a private charter program under § 1544.101(f), or a full all-cargo program under § 1544.101(h) and (i), each aircraft operator must—

(1) Arrange with TSA and the airport operator, as appropriate, for law enforcement personnel meeting the qualifications and standards specified in § 1542.217 of this chapter to be available to respond to incidents, and

(2) Provide its employees, including crewmembers, current information regarding procedures for obtaining law enforcement assistance at that airport.

[67 FR 8364, Feb. 22, 2002, as amended at 71 FR 30510, May 26, 2006]

§ 1544.219 Carriage of accessible weapons.

(a) *Flights for which screening is conducted.* The provisions of § 1544.201(d), with respect to accessible weapons, do not apply to a law enforcement officer (LEO) aboard a flight for which screening is required if the requirements of this section are met. Paragraph (a) of this section does not apply to a Federal Air Marshal on duty status under § 1544.223.

(1) Unless otherwise authorized by TSA, the armed LEO must meet the following requirements:

(i) Be a Federal law enforcement officer or a full-time municipal, county, or state law enforcement officer who is a direct employee of a government agency.

(ii) Be sworn and commissioned to enforce criminal statutes or immigration statutes.

(iii) Be authorized by the employing agency to have the weapon in connection with assigned duties.

(iv) Has completed the training program ''Law Enforcement Officers Flying Armed.''

(2) In addition to the requirements of paragraph (a)(1) of this section, the armed LEO must have a need to have the weapon accessible from the time he or she would otherwise check the weapon until the time it would be claimed after deplaning. The need to have the weapon accessible must be determined by the employing agency, department, or service and be based on one of the following:

(i) The provision of protective duty, for instance, assigned to a principal or advance team, or on travel required to be prepared to engage in a protective function.

(ii) The conduct of a hazardous surveillance operation.

(iii) On official travel required to report to another location, armed and prepared for duty.

(iv) Employed as a Federal LEO, whether or not on official travel, and armed in accordance with an agency-wide policy governing that type of travel established by the employing agency by directive or policy statement.

(v) Control of a prisoner, in accordance with §1544.221, or an armed LEO on a round trip ticket returning from escorting, or traveling to pick up, a prisoner.

(vi) TSA Federal Air Marshal on duty status.

(3) The armed LEO must comply with the following notification requirements:

(i) All armed LEOs must notify the aircraft operator of the flight(s) on which he or she needs to have the weapon accessible at least 1 hour, or in an emergency as soon as practicable, before departure.

(ii) Identify himself or herself to the aircraft operator by presenting credentials that include a clear full-face picture, the signature of the armed LEO, and the signature of the authorizing official of the agency, service, or department or the official seal of the agency, service, or department. A badge, shield, or similar device may not be used, or accepted, as the sole means of identification.

(iii) If the armed LEO is a State, county, or municipal law enforcement officer, he or she must present an original letter of authority, signed by an authorizing official from his or her employing agency, service or department, confirming the need to travel armed and detailing the itinerary of the travel while armed.

(iv) If the armed LEO is an escort for a foreign official then this paragraph (a)(3) may be satisfied by a State Department notification.

(4) The aircraft operator must do the following:

(i) Obtain information or documentation required in paragraphs (a)(3)(ii), (iii), and (iv) of this section.

(ii) Advise the armed LEO, before boarding, of the aircraft operator's procedures for carrying out this section.

(iii) Have the LEO confirm he/she has completed the training program ''Law Enforcement Officers Flying Armed'' as required by TSA, unless otherwise authorized by TSA.

(iv) Ensure that the identity of the armed LEO is known to the appropriate personnel who are responsible for security during the boarding of the aircraft.

(v) Notify the pilot in command and other appropriate crewmembers, of the location of each armed LEO aboard the aircraft. Notify any other armed LEO of the location of each armed LEO, including FAM's. Under circumstances described in the security program, the aircraft operator must not close the doors until the notification is complete.

(vi) Ensure that the information required in paragraphs (a)(3)(i) and (ii) of this section is furnished to the flight crew of each additional connecting flight by the Ground Security Coordinator or other designated agent at each location.

(b) *Flights for which screening is not conducted.* The provisions of §1544.201(d), with respect to accessible weapons, do not apply to a LEO aboard a flight for which screening is not required if the requirements of paragraphs (a)(1), (3), and (4) of this section are met.

(c) *Alcohol.* (1) No aircraft operator may serve any alcoholic beverage to an armed LEO.

(2) No armed LEO may:

(i) Consume any alcoholic beverage while aboard an aircraft operated by an aircraft operator.

(ii) Board an aircraft armed if they have consumed an alcoholic beverage within the previous 8 hours.

(d) *Location of weapon.* (1) Any individual traveling aboard an aircraft while armed must at all times keep their weapon:

(i) Concealed and out of view, either on their person or in immediate reach, if the armed LEO is not in uniform.

(ii) On their person, if the armed LEO is in uniform.

(2) No individual may place a weapon in an overhead storage bin.

§ 1544.221 Carriage of prisoners under the control of armed law enforcement officers.

(a) This section applies as follows:

(1) This section applies to the transport of prisoners under the escort of an armed law enforcement officer.

(2) This section does not apply to the carriage of passengers under voluntary protective escort.

(3) This section does not apply to the escort of non-violent detainees of the Immigration and Naturalization Service. This section does not apply to individuals who may be traveling with a prisoner and armed escort, such as the family of a deportee who is under armed escort.

(b) For the purpose of this section:

(1) ''High risk prisoner'' means a prisoner who is an exceptional escape risk, as determined by the law enforcement agency, and charged with, or convicted of, a violent crime.

(2) ''Low risk prisoner'' means any prisoner who has not been designated as ''high risk.''

(c) No aircraft operator may carry a prisoner in the custody of an armed law enforcement officer aboard an aircraft for which screening is required unless, in addition to the requirements in § 1544.219, the following requirements are met:

(1) The agency responsible for control of the prisoner has determined whether the prisoner is considered a high risk or a low risk.

(2) Unless otherwise authorized by TSA, no more than one high risk prisoner may be carried on the aircraft.

(d) No aircraft operator may carry a prisoner in the custody of an armed law enforcement officer aboard an aircraft for which screening is required unless the following staffing requirements are met:

(1) A minimum of one armed law enforcement officer must control a low risk prisoner on a flight that is scheduled for 4 hours or less. One armed law enforcement officer may control no more than two low risk prisoners.

(2) A minimum of two armed law enforcement officers must control a low risk prisoner on a flight that is scheduled for more than 4 hours. Two armed law enforcement officers may control no more than two low risk prisoners.

(3) For high-risk prisoners:

(i) For one high-risk prisoner on a flight: A minimum of two armed law enforcement officers must control a high risk prisoner. No other prisoners may be under the control of those two armed law enforcement officers.

(ii) If TSA has authorized more than one high-risk prisoner to be on the flight under paragraph (c)(2) of this section, a minimum of one armed law enforcement officer for each prisoner and one additional armed law enforcement officer must control the prisoners. No other prisoners may be under the control of those armed law enforcement officers.

(e) An armed law enforcement officer who is escorting a prisoner—

(1) Must notify the aircraft operator at least 24 hours before the scheduled departure, or, if that is not possible as far in advance as possible of the following—

(i) The identity of the prisoner to be carried and the flight on which it is proposed to carry the prisoner; and

(ii) Whether or not the prisoner is considered to be a high risk or a low risk.

(2) Must arrive at the check-in counter at least 1 hour before to the scheduled departure.

(3) Must assure the aircraft operator, before departure, that each prisoner under the control of the officer(s) has been searched and does not have on or about his or her person or property anything that can be used as a weapon.

(4) Must be seated between the prisoner and any aisle.

(5) Must accompany the prisoner at all times, and keep the prisoner under control while aboard the aircraft.

(f) No aircraft operator may carry a prisoner in the custody of an armed law enforcement officer aboard an aircraft unless the following are met:

(1) When practicable, the prisoner must be boarded before any other boarding passengers and deplaned after all other deplaning passengers.

(2) The prisoner must be seated in a seat that is neither located in any passenger lounge area nor located next to or directly across from any exit and, when practicable, the aircraft operator should seat the prisoner in the rearmost seat of the passenger cabin.

(g) Each armed law enforcement officer escorting a prisoner and each aircraft operator must ensure that the prisoner is restrained from full use of his or her hands by an appropriate device that provides for minimum movement of the prisoner's hands, and must ensure that leg irons are not used.

(h) No aircraft operator may provide a prisoner under the control of a law enforcement officer—

(1) With food or beverage or metal eating utensils unless authorized to do so by the armed law enforcement officer.

(2) With any alcoholic beverage.

§ 1544.223 Transportation of Federal Air Marshals.

(a) A Federal Air Marshal on duty status may have a weapon accessible while aboard an aircraft for which screening is required.

(b) Each aircraft operator must carry Federal Air Marshals, in the number and manner specified by TSA, on each scheduled passenger operation, and public charter passenger operation designated by TSA.

(c) Each Federal Air Marshal must be carried on a first priority basis and without charge while on duty, including positioning and repositioning flights. When a Federal Air Marshal is assigned to a scheduled flight that is canceled for any reason, the aircraft operator must carry that Federal Air Marshal without charge on another flight as designated by TSA.

(d) Each aircraft operator must assign the specific seat requested by a Federal Air Marshal who is on duty status. If another LEO is assigned to that seat or requests that seat, the aircraft operator must inform the Federal Air Marshal. The Federal Air Marshal will coordinate seat assignments with the other LEO.

(e) The Federal Air Marshal identifies himself or herself to the aircraft operator by presenting credentials that include a clear, full-face picture, the signature of the Federal Air Marshal, and the signature of the FAA Administrator. A badge, shield, or similar device may not be used or accepted as the sole means of identification.

(f) The requirements of §1544.219(a) do not apply for a Federal Air Marshal on duty status.

(g) Each aircraft operator must restrict any information concerning the presence, seating, names, and purpose of Federal Air Marshals at any station or on any flight to those persons with an operational need to know.

(h) Law enforcement officers authorized to carry a weapon during a flight will be contacted directly by a Federal Air Marshal who is on that same flight.

§ 1544.225 Security of aircraft and facilities.

Each aircraft operator must use the procedures included, and the facilities and equipment described, in its security program to perform the following control functions with respect to each aircraft operation:

(a) Prevent unauthorized access to areas controlled by the aircraft operator under an exclusive area agreement in accordance with §1542.111 of this chapter.

(b) Prevent unauthorized access to each aircraft.

(c) Conduct a security inspection of each aircraft before placing it into passenger operations if access has not been controlled in accordance with the aircraft operator security program and as otherwise required in the security program.

(d) When operating under a full program or a full all-cargo program, prevent unauthorized access to the operational area of the aircraft while loading or unloading cargo.

[67 FR 8364, Feb. 22, 2002, as amended at 71 FR 30510, May 26, 2006]

§ 1544.227 Exclusive area agreement.

(a) An aircraft operator that has entered into an exclusive area agreement with an airport operator, under §1542.111 of this chapter must carry out that exclusive area agreement.

(b) The aircraft operator must list in its security program the locations at which it has entered into exclusive area agreements with an airport operator.

(c) The aircraft operator must provide the exclusive area agreement to TSA upon request.

(d) Any exclusive area agreements in effect on November 14, 2001, must meet the requirements of this section and §1542.111 of this chapter no later than November 14, 2002.

§ 1544.228 Access to cargo: Security threat assessments for cargo personnel in the United States.

This section applies in the United States to each aircraft operator operating under a full program under §1544.101(a), or a full all-cargo program under §1544.101(h) of this part.

(a) This section applies for each employee and agent the aircraft operator authorizes to have unescorted access to cargo from the time—

(1) The cargo reaches a location where an aircraft operator with a full all-cargo program consolidates or inspects it pursuant to security program requirements until the cargo enters an airport Security Identification Display Area or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier; or

(2) An aircraft operator with a full program accepts the cargo until the cargo:

(i) Enters an airport Security Identification Display Area;

(ii) Is removed from the destination airport; or

(iii) Is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier.

(b) Before an aircraft operator authorizes, and before an employee or agent gains, unescorted access to cargo as described in paragraph (a) of this section, each employee or agent must successfully complete one of the following:

(1) A criminal history records check under §§1542.209, 1544.229, or 1544.230 of this chapter, if the employee or agent is otherwise required to undergo that check.

(2) A Security Threat Assessment under part 1540 subpart C of this chapter. An employee or agent who has successfully completed this Security Threat Assessment for one employer need not complete it for another employer if the employee or agent has been continuously employed in a position that requires a Security Threat Assessment.

(3) Another Security Threat Assessment approved by TSA as comparable to paragraphs (b)(1) or (2) of this section.

(c) Each aircraft operator must ensure that each individual who has access to its cargo—

(1) Has successfully completed one of the checks in paragraph (b) of this section;

(2) Is escorted by an employee or agent who has successfully completed one of the checks in paragraph (b) of this section; or

(3) Is authorized to serve as law enforcement personnel at that location.

(d) Operators must submit to TSA the names and other identifying information required by TSA of all individuals required to successfully complete an assessment under paragraph (b) not later than May 15, 2007, for direct employees and not later than July 15, 2007, for agents. After those dates, the operators may not allow an individual to perform a function for which a STA is required, unless the operator has submitted the information for that individual to TSA.

(e) Operators must comply with the requirements of paragraphs (a), (b), and (c) of this section not later than the dates to be specified by TSA in a future rule in the FEDERAL REGISTER.

[71 FR 30511, May 26, 2006; 71 FR 31964, June 2, 2006 as amended at 71 FR 62549, Oct. 25, 2006; 72 FR 13025, Mar. 20, 2007]

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, §1544.228 was revised, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1544.228 Access to cargo and cargo screening: Security threat assessments for cargo personnel in the United States.

This section applies in the United States to each aircraft operator operating under a full program under §1544.101(a) or a full all-cargo program under §1544.101(h).

(a) Before an aircraft operator authorizes and before an individual performs a function described in paragraph (b) of this section—

(1) Each individual must successfully complete a security threat assessment or comparable security threat assessment described in part 1540 subpart C of this chapter; and

(2) Each aircraft operator must complete the requirements in part 1540 subpart C.

(b) The security threat assessment required in paragraph (a) of this section applies to the following:

(1) Each individual who has unescorted access to cargo and access to information that such cargo will be transported on a passenger aircraft; or who has unescorted access to cargo that has been screened for transport on a passenger aircraft; or who performs certain functions related to the transportation, dispatch, or security of cargo for transport on a passenger aircraft or all-cargo aircraft, as specified in the aircraft operator's security program; from the time—

(i) The cargo reaches a location where an aircraft operator with a full all-cargo program consolidates or inspects it pursuant to security program requirements until the cargo enters an airport Security Identification Display Area or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier; or

(ii) An aircraft operator with a full program accepts the cargo until the cargo—

(A) Enters an airport Security Identification Display Area;

(B) Is removed from the destination airport; or

(C) Is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier.

(2) Each individual the aircraft operator authorizes to screen cargo or to supervise the screening of cargo under §1544.205.

§1544.229 Fingerprint-based criminal history records checks (CHRC): Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions.

This section applies to each aircraft operator operating under a full program, a private charter program, or a full all-cargo program.

(a) *Scope.* The following individuals are within the scope of this section. Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions, are collectively referred to as ''covered functions.''

(1) *New unescorted access authority or authority to perform screening functions.* (i) Each employee or contract employee covered under a certification made to an airport operator on or after December 6, 2001, pursuant to 14 CFR 107.209(n) in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001) or §1542.209(n) of this chapter.

(ii) Each individual issued on or after December 6, 2001, an aircraft operator identification media that one or more airports accepts as airport-approved media for unescorted access authority within a security identification display area (SIDA), as described in §1542.205 of this chapter (referred to as ''unescorted access authority'').

(iii) Each individual granted authority to perform the following screening functions at locations within the United States (referred to as ''authority to perform screening functions''):

(A) Screening passengers or property that will be carried in a cabin of an aircraft of an aircraft operator required to screen passengers under this part.

(B) Serving as an immediate supervisor (checkpoint security supervisor (CSS)), and the next supervisory level (shift or site supervisor), to those individuals described in paragraphs (a)(1)(iii)(A) or (a)(1)(iii)(C) of this section.

(C) Screening cargo that will be carried on an aircraft of an aircraft operator with a full all-cargo program.

(2) *Current unescorted access authority or authority to perform screening functions.* (i) Each employee or contract employee covered under a certification made to an airport operator pursuant to 14 CFR 107.31(n) in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001), or pursuant to 14 CFR 107.209(n) in effect prior to December 6, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001).

(ii) Each individual who holds on December 6, 2001, an aircraft operator identification media that one or more airports accepts as airport-approved media for unescorted access authority within a security identification display area (SIDA), as described in §1542.205 of this chapter.

(iii) Each individual who is performing on December 6, 2001, a screening function identified in paragraph (a)(1)(iii) of this section.

(3) *New authority to perform checked baggage or cargo functions.* Each individual who, on and after February 17, 2002, is granted the authority to perform the following checked baggage and cargo functions (referred to as ''authority to perform checked baggage or cargo functions''), except for individuals described in paragraph (a)(1) of this section:

(i) Screening of checked baggage or cargo of an aircraft operator required to screen passengers under this part, or serving as an immediate supervisor of such an individual.

(ii) Accepting checked baggage for transport on behalf of an aircraft operator required to screen passengers under this part.

(4) *Current authority to perform checked baggage or cargo functions.* Each individual who holds on February 17, 2002, authority to perform checked baggage or cargo functions, except for individuals described in paragraph (a)(1) or (2) of this section.

(b) *Individuals seeking unescorted access authority, authority to perform screening functions, or authority to perform checked baggage or cargo functions.* Each aircraft operator must ensure that each individual identified in paragraph (a)(1) or (3) of this section has undergone a fingerprint-based CHRC that does not disclose that he or she has a disqualifying criminal offense, as described in paragraph (d) of this section, before—

(1) Making a certification to an airport operator regarding that individual;

(2) Issuing an aircraft operator identification medium to that individual;

(3) Authorizing that individual to perform screening functions; or

(4) Authorizing that individual to perform checked baggage or cargo functions.

(c) *Individuals who have not had a CHRC*—(1) *Deadline for conducting a CHRC.* Each aircraft operator must ensure that, on and after December 6, 2002:

(i) No individual retains unescorted access authority, whether obtained as a result of a certification to an airport operator under 14 CFR 107.31(n) in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001), or under 14 CFR 107.209(n) in effect prior to December 6, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001), or obtained as a result of the issuance of an aircraft operator's identification media, unless the individual has been subject to a fingerprint-based CHRC for unescorted access authority under this part.

(ii) No individual continues to have authority to perform screening functions described in paragraph (a)(1)(iii) of this section, unless the individual has been subject to a fingerprint-based CHRC under this part.

(iii) No individual continues to have authority to perform checked baggage or cargo functions described in paragraph (a)(3) of this section, unless the individual has been subject to a fingerprint-based CHRC under this part.

(2) *Lookback for individuals with unescorted access authority or authority to perform screening functions.* When a CHRC discloses a disqualifying criminal offense for which the conviction or finding was on or after December 6, 1991, the aircraft operator must immediately suspend that individual's unescorted access authority or authority to perform screening functions.

(3) *Lookback for individuals with authority to perform checked baggage or cargo functions.* When a CHRC discloses a disqualifying criminal offense for which the conviction or finding was on or after February 17, 1992, the aircraft operator must immediately suspend that individual's authority to perform checked baggage or cargo functions.

(d) *Disqualifying criminal offenses.* An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty by reason of insanity, of any of the disqualifying crimes listed in this paragraph in any jurisdiction during the 10 years before the date of the individual's application for authority to perform covered functions, or while the individual has authority to perform covered functions. The disqualifying criminal offenses are as follows:

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.

(2) Interference with air navigation; 49 U.S.C. 46308.

(3) Improper transportation of a hazardous material; 49 U.S.C. 46312.

(4) Aircraft piracy; 49 U.S.C. 46502.

(5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504.

(6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.

(7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.

(8) Conveying false information and threats; 49 U.S.C. 46507.

(9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).

(10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.

(11) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.

(12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.

(13) Murder.

(14) Assault with intent to murder.

(15) Espionage.

(16) Sedition.

(17) Kidnapping or hostage taking.

(18) Treason.

(19) Rape or aggravated sexual abuse.

(20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.

(21) Extortion.

(22) Armed or felony unarmed robbery.

(23) Distribution of, or intent to distribute, a controlled substance.

(24) Felony arson.

(25) Felony involving a threat.

(26) Felony involving—

(i) Willful destruction of property;

(ii) Importation or manufacture of a controlled substance;

(iii) Burglary;

(iv) Theft;

(v) Dishonesty, fraud, or misrepresentation;

(vi) Possession or distribution of stolen property;

(vii) Aggravated assault;

(viii) Bribery; or

(ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

(27) Violence at international airports; 18 U.S.C. 37.

(28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d).

(e) *Fingerprint application and processing.* (1) At the time of fingerprinting, the aircraft operator must provide the individual to be fingerprinted a fingerprint application that includes only the following—

(i) The disqualifying criminal offenses described in paragraph (d) of this section.

(ii) A statement that the individual signing the application does not have a disqualifying criminal offense.

(iii) A statement informing the individual that Federal regulations under 49 CFR 1544.229 impose a continuing obligation to disclose to the aircraft operator within 24 hours if he or she is convicted of any disqualifying criminal offense that occurs while he or she has authority to perform a covered function.

(iv) A statement reading, ''The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or both. (See section 1001 of Title 18 United States Code.)''

(v) A line for the printed name of the individual.

(vi) A line for the individual's signature and date of signature.

(2) Each individual must complete and sign the application prior to submitting his or her fingerprints.

(3) The aircraft operator must verify the identity of the individual through two forms of identification prior to fingerprinting, and ensure that the printed name on the fingerprint application is legible. At least one of the two forms of identification must have been issued by a government authority, and at least one must include a photo.

(4) The aircraft operator must:

(i) Advise the individual that a copy of the criminal record received from the FBI will be provided to the individual, if requested by the individual in writing; and

(ii) Identify a point of contact if the individual has questions about the results of the CHRC.

(5) The aircraft operator must collect, control, and process one set of legible and classifiable fingerprints under direct observation by the aircraft operator or a law enforcement officer.

(6) Fingerprints may be obtained and processed electronically, or recorded

on fingerprint cards approved by the FBI and distributed by TSA for that purpose.

(7) The fingerprint submission must be forwarded to TSA in the manner specified by TSA.

(f) *Fingerprinting fees.* Aircraft operators must pay for all fingerprints in a form and manner approved by TSA. The payment must be made at the designated rate (available from the local TSA security office) for each set of fingerprints submitted. Information about payment options is available though the designated TSA headquarters point of contact. Individual personal checks are not acceptable.

(g) *Determination of arrest status.* (1) When a CHRC on an individual described in paragraph (a)(1) or (3) of this section discloses an arrest for any disqualifying criminal offense listed in paragraph (d) of this section without indicating a disposition, the aircraft operator must determine, after investigation, that the arrest did not result in a disqualifying offense before granting authority to perform a covered function. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(2) When a CHRC on an individual described in paragraph (a)(2) or (4) of this section discloses an arrest for any disqualifying criminal offense without indicating a disposition, the aircraft operator must suspend the individual's authority to perform a covered function not later than 45 days after obtaining the CHRC unless the aircraft operator determines, after investigation, that the arrest did not result in a disqualifying criminal offense. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(3) The aircraft operator may only make the determinations required in paragraphs (g)(1) and (g)(2) of this section for individuals for whom it is issuing, or has issued, authority to perform a covered function; and individuals who are covered by a certification from an aircraft operator under §1542.209(n) of this chapter. The aircraft operator may not make determinations for individuals described in §1542.209(a) of this chapter.

(h) *Correction of FBI records and notification of disqualification.* (1) Before making a final decision to deny authority to an individual described in paragraph (a)(1) or (3) of this section, the aircraft operator must advise him or her that the FBI criminal record discloses information that would disqualify him or her from receiving or retaining authority to perform a covered function and provide the individual with a copy of the FBI record if he or she requests it.

(2) The aircraft operator must notify an individual that a final decision has been made to grant or deny authority to perform a covered function.

(3) Immediately following the suspension of authority to perform a covered function, the aircraft operator must advise the individual that the FBI criminal record discloses information that disqualifies him or her from retaining his or her authority, and provide the individual with a copy of the FBI record if he or she requests it.

(i) *Corrective action by the individual.* The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record, subject to the following conditions—

(1) For an individual seeking unescorted access authority or authority to perform screening functions on or after December 6, 2001; or an individual seeking authority to perform checked baggage or cargo functions on or after February 17, 2002; the following applies:

(i) Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the aircraft operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The aircraft operator must obtain a copy, or accept a copy from the individual, of the revised FBI record or a certified true copy of the information

from the appropriate court, prior to authority to perform a covered function.

(ii) If no notification, as described in paragraph (h)(1) of this section, is received within 30 days, the aircraft operator may make a final determination to deny authority to perform a covered function.

(2) For an individual with unescorted access authority or authority to perform screening functions before December 6, 2001; or an individual with authority to perform checked baggage or cargo functions before February 17, 2002; the following applies: Within 30 days after being advised of suspension because the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the aircraft operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The aircraft operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to reinstating authority to perform a covered function.

(j) *Limits on dissemination of results.* Criminal record information provided by the FBI may be used only to carry out this section and §1542.209 of this chapter. No person may disseminate the results of a CHRC to anyone other than:

(1) The individual to whom the record pertains, or that individual's authorized representative.

(2) Officials of airport operators who are determining whether to grant unescorted access to the individual under part 1542 of this chapter when the determination is not based on the aircraft operator's certification under §1542.209(n) of this chapter.

(3) Other aircraft operators who are determining whether to grant authority to perform a covered function under this part.

(4) Others designated by TSA.

(k) *Recordkeeping.* The aircraft operator must maintain the following information.

(1) *Investigation conducted before December 6, 2001.* The aircraft operator must maintain and control the access or employment history investigation files, including the criminal history records results portion, for investigations conducted before December 6, 2001.

(2) *Fingerprint application process on or after December 6, 2001.* The aircraft operator must physically maintain, control, and, as appropriate, destroy the fingerprint application and the criminal record. Only direct aircraft operator employees may carry out the responsibility for maintaining, controlling, and destroying criminal records.

(3) *Protection of records—all investigations.* The records required by this section must be maintained in a manner that is acceptable to TSA and in a manner that protects the confidentiality of the individual.

(4) *Duration—all investigations.* The records identified in this section with regard to an individual must be maintained until 180 days after the termination of the individual's authority to perform a covered function. When files are no longer maintained, the criminal record must be destroyed.

(l) *Continuing responsibilities.* (1) Each individual with unescorted access authority or the authority to perform screening functions on December 6, 2001, who had a disqualifying criminal offense in paragraph (d) of this section on or after December 6, 1991, must, by January 7, 2002, report the conviction to the aircraft operator and surrender the SIDA access medium to the issuer and cease performing screening functions, as applicable.

(2) Each individual with authority to perform a covered function who has a disqualifying criminal offense must report the offense to the aircraft operator and surrender the SIDA access medium to the issuer within 24 hours of the conviction or the finding of not guilty by reason of insanity.

(3) If information becomes available to the aircraft operator indicating that an individual with authority to perform a covered function has a possible conviction for any disqualifying criminal offense in paragraph (d) of this section, the aircraft operator must determine the status of the conviction. If a disqualifying criminal offense is confirmed the aircraft operator must immediately revoke any authority to perform a covered function.

(4) Each individual with authority to perform checked baggage or cargo functions on February 17, 2002, who had a disqualifying criminal offense in paragraph (d) of this section on or after February 17, 1992, must, by March 25 2002, report the conviction to the aircraft operator and cease performing check baggage or cargo functions.

(m) *Aircraft operator responsibility*. The aircraft operator must—

(1) Designate an individual(s) to be responsible for maintaining and controlling the employment history investigations for those whom the aircraft operator has made a certification to an airport operator under 14 CFR 107.209(n) in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001), and for those whom the aircraft operator has issued identification media that are airport-accepted. The aircraft operator must designate a direct employee to maintain, control, and, as appropriate, destroy criminal records.

(2) Designate an individual(s) to maintain the employment history investigations of individuals with authority to perform screening functions whose files must be maintained at the location or station where the screener is performing his or her duties.

(3) Designate an individual(s) at appropriate locations to serve as the contact to receive notification from individuals seeking authority to perform covered functions of their intent to seek correction of their FBI criminal record.

(4) Audit the employment history investigations performed in accordance with this section and 14 CFR 108.33 in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001). The aircraft operator must set forth the audit procedures in its security program.

[67 FR 8364, Feb. 22, 2002, as amended at 71 FR 30511, May 26, 2006]

§ 1544.230 Fingerprint-based criminal history records checks (CHRC): Flightcrew members.

(a) *Scope*. This section applies to each flightcrew member for each aircraft operator, except that this section does not apply to flightcrew members who are subject to § 1544.229.

(b) *CHRC required*. Each aircraft operator must ensure that each flightcrew member has undergone a fingerprint-based CHRC that does not disclose that he or she has a disqualifying criminal offense, as described in § 1544.229(d), before allowing that individual to serve as a flightcrew member.

(c) *Application and fees*. Each aircraft operator must ensure that each flightcrew member's fingerprints are obtained and submitted as described in § 1544.229 (e) and (f).

(d) *Determination of arrest status*. (1) When a CHRC on an individual described in paragraph (a) of this section discloses an arrest for any disqualifying criminal offense listed in § 1544.229(d) without indicating a disposition, the aircraft operator must determine, after investigation, that the arrest did not result in a disqualifying offense before the individual may serve as a flightcrew member. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in § 1544.229(d), the flight crewmember is not disqualified under this section.

(2) When a CHRC on an individual described in paragraph (a) of this section discloses an arrest for any disqualifying criminal offense listed in § 1544.229(d) without indicating a disposition, the aircraft operator must suspend the individual's flightcrew member privileges not later than 45 days after obtaining a CHRC, unless the aircraft operator determines, after investigation, that the arrest did not result in a disqualifying criminal offense. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in § 1544.229(d), the flight crewmember is not disqualified under this section.

(3) The aircraft operator may only make the determinations required in paragraphs (d)(1) and (d)(2) of this section for individuals whom it is using, or will use, as a flightcrew member. The aircraft operator may not make determinations for individuals described in § 1542.209(a) of this chapter.

(e) *Correction of FBI records and notification of disqualification*. (1) Before

making a final decision to deny the individual the ability to serve as a flightcrew member, the aircraft operator must advise the individual that the FBI criminal record discloses information that would disqualify the individual from serving as a flightcrew member and provide the individual with a copy of the FBI record if the individual requests it.

(2) The aircraft operator must notify the individual that a final decision has been made to allow or deny the individual flightcrew member status.

(3) Immediately following the denial of flightcrew member status, the aircraft operator must advise the individual that the FBI criminal record discloses information that disqualifies him or her from retaining his or her flightcrew member status, and provide the individual with a copy of the FBI record if he or she requests it.

(f) *Corrective action by the individual.* The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record, subject to the following conditions—

(1) Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the aircraft operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The aircraft operator must obtain a copy, or accept a copy from the individual, of the revised FBI record or a certified true copy of the information from the appropriate court, prior to allowing the individual to serve as a flightcrew member.

(2) If no notification, as described in paragraph (f)(1) of this section, is received within 30 days, the aircraft operator may make a final determination to deny the individual flightcrew member status.

(g) *Limits on the dissemination of results.* Criminal record information provided by the FBI may be used only to carry out this section. No person may disseminate the results of a CHRC to anyone other than—

(1) The individual to whom the record pertains, or that individual's authorized representative.

(2) Others designated by TSA.

(h) *Recordkeeping*—(1) *Fingerprint application process.* The aircraft operator must physically maintain, control, and, as appropriate, destroy the fingerprint application and the criminal record. Only direct aircraft operator employees may carry out the responsibility for maintaining, controlling, and destroying criminal records.

(2) *Protection of records.* The records required by this section must be maintained by the aircraft operator in a manner that is acceptable to TSA that protects the confidentiality of the individual.

(3) *Duration.* The records identified in this section with regard to an individual must be made available upon request by TSA, and maintained by the aircraft operator until 180 days after the termination of the individual's privileges to perform flightcrew member duties with the aircraft operator. When files are no longer maintained, the aircraft operator must destroy the CHRC results.

(i) *Continuing responsibilities.* (1) Each flightcrew member identified in paragraph (a) of this section who has a disqualifying criminal offense must report the offense to the aircraft operator within 24 hours of the conviction or the finding of not guilty by reason of insanity.

(2) If information becomes available to the aircraft operator indicating that a flightcrew member identified in paragraph (a) of this section has a possible conviction for any disqualifying criminal offense in §1544.229 (d), the aircraft operator must determine the status of the conviction. If a disqualifying criminal offense is confirmed, the aircraft operator may not assign that individual to flightcrew duties in operations identified in paragraph (a).

(j) *Aircraft operator responsibility.* The aircraft operator must—(1) Designate a direct employee to maintain, control, and, as appropriate, destroy criminal records.

(2) Designate an individual(s) to maintain the CHRC results.

(3) Designate an individual(s) at appropriate locations to receive notification from individuals of their intent to seek correction of their FBI criminal record.

(k) *Compliance date.* Each aircraft operator must comply with this section for each flightcrew member described in paragraph (a) of this section not later than December 6, 2002.

[67 FR 8209, Feb. 22, 2002]

§ 1544.231 Airport-approved and exclusive area personnel identification systems.

(a) Each aircraft operator must establish and carry out a personnel identification system for identification media that are airport-approved, or identification media that are issued for use in an exclusive area. The system must include the following:

(1) Personnel identification media that—

(i) Convey a full face image, full name, employer, and identification number of the individual to whom the identification medium is issued;

(ii) Indicate clearly the scope of the individual's access and movement privileges;

(iii) Indicate clearly an expiration date; and

(iv) Are of sufficient size and appearance as to be readily observable for challenge purposes.

(2) Procedures to ensure that each individual in the secured area or SIDA continuously displays the identification medium issued to that individual on the outermost garment above waist level, or is under escort.

(3) Procedures to ensure accountability through the following:

(i) Retrieving expired identification media.

(ii) Reporting lost or stolen identification media.

(iii) Securing unissued identification media stock and supplies.

(iv) Auditing the system at a minimum of once a year, or sooner, as necessary to ensure the integrity and accountability of all identification media.

(v) As specified in the aircraft operator security program, revalidate the identification system or reissue identification media if a portion of all issued, unexpired identification media are lost, stolen, or unretrieved, including identification media that are combined with access media.

(vi) Ensure that only one identification medium is issued to an individual at a time. A replacement identification medium may only be issued if an individual declares in writing that the medium has been lost or stolen.

(b) The aircraft operator may request approval of a temporary identification media system that meets the standards in §1542.211(b) of this chapter, or may arrange with the airport to use temporary airport identification media in accordance with that section.

(c) Each aircraft operator must submit a plan to carry out this section to TSA no later than May 13, 2002. Each aircraft operator must fully implement its plan no later than November 14, 2003.

§ 1544.233 Security coordinators and crewmembers, training.

(a) No aircraft operator may use any individual as a Ground Security Coordinator unless, within the preceding 12-calendar months, that individual has satisfactorily completed the security training as specified in the aircraft operator's security program.

(b) No aircraft operator may use any individual as an in-flight security coordinator or crewmember on any domestic or international flight unless, within the preceding 12-calendar months or within the time period specified in an Advanced Qualifications Program approved under SFAR 58 in 14 CFR part 121, that individual has satisfactorily completed the security training required by 14 CFR 121.417(b)(3)(v) or 135.331(b)(3)(v), and as specified in the aircraft operator's security program.

(c) With respect to training conducted under this section, whenever an individual completes recurrent training within one calendar month earlier, or one calendar month after the date it was required, that individual is considered to have completed the training in the calendar month in which it was required.

§ 1544.235 Training and knowledge for individuals with security-related duties.

(a) No aircraft operator may use any direct or contractor employee to perform any security-related duties to meet the requirements of its security

program unless that individual has received training as specified in its security program including their individual responsibilities in §1540.105 of this chapter.

(b) Each aircraft operator must ensure that individuals performing security-related duties for the aircraft operator have knowledge of the provisions of this part, applicable Security Directives and Information Circulars, the approved airport security program applicable to their location, and the aircraft operator's security program to the extent that such individuals need to know in order to perform their duties.

§1544.237 Flight deck privileges.

(a) For each aircraft that has a door to the flight deck, each aircraft operator must restrict access to the flight deck as provided in its security program.

(b) This section does not restrict access for an FAA air carrier inspector, an authorized representative of the National Transportation Safety Board, or for an Agent of the United States Secret Service, under 14 CFR parts 121, 125, or 135. This section does not restrict access for a Federal Air Marshal under this part.

[67 FR 8210, Feb. 22, 2002]

§1544.239 Known shipper program.

This section applies to each aircraft operator operating under a full program under §1544.101(a) of this part and to each aircraft operator with a TSA security program approved for transfer of cargo to an aircraft operator with a full program or a foreign air carrier under paragraphs §1546.101(a) or (b) of this chapter.

(a) For cargo to be loaded on its aircraft in the United States, each aircraft operator must have and carry out a known shipper program in accordance with its security program. The program must—

(1) Determine the shipper's validity and integrity as provided in the security program;

(2) Provide that the aircraft operator will separate known shipper cargo from unknown shipper cargo; and

(3) Provide for the aircraft operator to ensure that cargo is screened or inspected as set forth in its security program.

(b) When required by TSA, each aircraft operator must submit in a form and manner acceptable to TSA—

(1) Information identified in its security program regarding a known shipper, or an applicant for that status; and

(2) Corrections and updates of this information upon learning of a change to the information specified in paragraph (b)(1) of this section.

[71 FR 30511, May 26, 2006]

Subpart D—Threat and Threat Response

§1544.301 Contingency plan.

Each aircraft operator must adopt a contingency plan and must:

(a) Implement its contingency plan when directed by TSA.

(b) Ensure that all information contained in the plan is updated annually and that appropriate persons are notified of any changes.

(c) Participate in an airport-sponsored exercise of the airport contingency plan or its equivalent, as provided in its security program.

§1544.303 Bomb or air piracy threats.

(a) *Flight: Notification.* Upon receipt of a specific and credible threat to the security of a flight, the aircraft operator must—

(1) Immediately notify the ground and in-flight security coordinators of the threat, any evaluation thereof, and any measures to be applied; and

(2) Ensure that the in-flight security coordinator notifies all crewmembers of the threat, any evaluation thereof, and any measures to be applied; and

(3) Immediately notify the appropriate airport operator.

(b) *Flight: Inspection.* Upon receipt of a specific and credible threat to the security of a flight, each aircraft operator must attempt to determine whether or not any explosive or incendiary is present by doing the following:

(1) Conduct a security inspection on the ground before the next flight or, if the aircraft is in flight, immediately after its next landing.

(2) If the aircraft is on the ground, immediately deplane all passengers

and submit that aircraft to a security search.

(3) If the aircraft is in flight, immediately advise the pilot in command of all pertinent information available so that necessary emergency action can be taken.

(c) *Ground facility.* Upon receipt of a specific and credible threat to a specific ground facility at the airport, the aircraft operator must:

(1) Immediately notify the appropriate airport operator.

(2) Inform all other aircraft operators and foreign air carriers at the threatened facility.

(3) Conduct a security inspection.

(d) *Notification.* Upon receipt of any bomb threat against the security of a flight or facility, or upon receiving information that an act or suspected act of air piracy has been committed, the aircraft operator also must notify TSA. If the aircraft is in airspace under other than U.S. jurisdiction, the aircraft operator must also notify the appropriate authorities of the State in whose territory the aircraft is located and, if the aircraft is in flight, the appropriate authorities of the State in whose territory the aircraft is to land. Notification of the appropriate air traffic controlling authority is sufficient action to meet this requirement.

§ 1544.305 Security Directives and Information Circulars.

(a) TSA may issue an Information Circular to notify aircraft operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(b) Each aircraft operator required to have an approved aircraft operator security program must comply with each Security Directive issued to the aircraft operator by TSA, within the time prescribed in the Security Directive for compliance.

(c) Each aircraft operator that receives a Security Directive must—

(1) Within the time prescribed in the Security Directive, verbally acknowledge receipt of the Security Directive to TSA.

(2) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(d) In the event that the aircraft operator is unable to implement the measures in the Security Directive, the aircraft operator must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval. The aircraft operator must submit the proposed alternative measures within the time prescribed in the Security Directive. The aircraft operator must implement any alternative measures approved by TSA.

(e) Each aircraft operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.

(f) Each aircraft operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular must:

(1) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need-to-know.

(2) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those with an operational need-to-know without the prior written consent of TSA.

Subpart E—Screener Qualifications When the Aircraft Operator Performs Screening

§ 1544.401 Applicability of this subpart.

(a) *Aircraft operator screening.* This subpart applies when the aircraft operator is conducting inspections as provided in § 1544.207(c).

(b) *Current screeners.* As used in this subpart, ''current screener'' means each individual who first performed screening functions before the date the aircraft operator must begin use of the

new screener training program provided by TSA. Until November 19, 2002, each current screener must comply with §1544.403. Until November 19, 2002, each aircraft operator must apply §1544.403 for each current screener. On and after November 19, 2002, each such current screener must comply with §§1544.405 through 1544.411, and each aircraft operator must comply with §§1544.405 through 1544.411 for such individuals.

(c) *New screeners.* As used in this subpart, ''new screener'' means each individual who first performs screening functions on and after the date the aircraft operator must begin use of the new screener training program provided by TSA. Each aircraft operator must apply §§1544.405 through 1544.411 for individuals who first perform screening functions for new screeners.

EFFECTIVE DATE NOTE: At 74 FR 47704, September 16, 2009, §1544.401 was revised, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1544.401 Applicability of this subpart.

This subpart applies when the aircraft operator is conducting inspections as provided in §1544.207.

§1544.403 Current screeners.

This section applies to current screeners. This section no longer applies on and after November 19, 2002.

(a) No aircraft operator may use any person to perform any screening function, unless that person has:

(1) A high school diploma, a General Equivalency Diploma, or a combination of education and experience that the aircraft operator has determined to have equipped the person to perform the duties of the position.

(2) Basic aptitudes and physical abilities including color perception, visual and aural acuity, physical coordination, and motor skills to the following standards:

(i) Screeners operating X-ray equipment must be able to distinguish on the X-ray monitor the appropriate imaging standard specified in the aircraft operator's security program. Wherever the X-ray system displays colors, the operator must be able to perceive each color;

(ii) Screeners operating any screening equipment must be able to distinguish each color displayed on every type of screening equipment and explain what each color signifies;

(iii) Screeners must be able to hear and respond to the spoken voice and to audible alarms generated by screening equipment in an active checkpoint environment;

(iv) Screeners performing physical searches or other related operations must be able to efficiently and thoroughly manipulate and handle such baggage, containers, and other objects subject to security processing; and

(v) Screeners who perform pat-downs or hand-held metal detector searches of persons must have sufficient dexterity and capability to thoroughly conduct those procedures over a person's entire body.

(3) The ability to read, speak, and write English well enough to—

(i) Carry out written and oral instructions regarding the proper performance of screening duties;

(ii) Read English language identification media, credentials, airline tickets, and labels on items normally encountered in the screening process;

(iii) Provide direction to and understand and answer questions from English-speaking persons undergoing screening; and

(iv) Write incident reports and statements and log entries into security records in the English language.

(4) Satisfactorily completed all initial, recurrent, and appropriate specialized training required by the aircraft operator's security program, except as provided in paragraph (b) of this section.

(b) The aircraft operator may use a person who has not completed the training required by paragraph (a)(4) of this section during the on-the-job portion of training to perform security functions provided that the person:

(1) Is closely supervised, and

(2) Does not make independent judgments as to whether persons or property may enter a sterile area or aircraft without further inspection.

(c) No aircraft operator must use a person to perform a screening function after that person has failed an operational test related to that function

until that person has successfully completed the remedial training specified in the aircraft operator's security program.

(d) Each aircraft operator must ensure that a Ground Security Coordinator conducts and documents an annual evaluation of each individual assigned screening duties and may continue that individual's employment in a screening capacity only upon the determination by the Ground Security Coordinator that the individual:

(1) Has not suffered a significant diminution of any physical ability required to perform a screening function since the last evaluation of those abilities;

(2) Has a satisfactory record of performance and attention to duty based on the standards and requirements in its security program; and

(3) Demonstrates the current knowledge and skills necessary to courteously, vigilantly, and effectively perform screening functions.

(e) Paragraphs (a) through (d) of this section do not apply to those screening functions conducted outside the United States over which the aircraft operator does not have operational control. In the event the aircraft operator is unable to implement paragraphs (a) through (d) of this section for screening functions outside the United States, the aircraft operator must notify TSA of those aircraft operator stations so affected.

(f) At locations outside the United States where the aircraft operator has operational control over a screening function, the aircraft operator may use screeners who do not meet the requirements of paragraph (a)(3) of this section, provided that at least one representative of the aircraft operator who has the ability to functionally read and speak English is present while the aircraft operator's passengers are undergoing security screening.

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, §1544.403 was removed and reserved, effective November 16, 2009.

§ 1544.405 New screeners: Qualifications of screening personnel.

(a) No individual subject to this subpart may perform a screening function unless that individual has the qualifications described in §§1544.405 through 1544.411. No aircraft operator may use such an individual to perform a screening function unless that person complies with the requirements of §§1544.405 through 1544.411.

(b) A screener must have a satisfactory or better score on a screener selection test administered by TSA.

(c) A screener must be a citizen of the United States.

(d) A screener must have a high school diploma, a General Equivalency Diploma, or a combination of education and experience that the TSA has determined to be sufficient for the individual to perform the duties of the position.

(e) A screener must have basic aptitudes and physical abilities including color perception, visual and aural acuity, physical coordination, and motor skills to the following standards:

(1) Screeners operating screening equipment must be able to distinguish on the screening equipment monitor the appropriate imaging standard specified in the aircraft operator's security program.

(2) Screeners operating any screening equipment must be able to distinguish each color displayed on every type of screening equipment and explain what each color signifies.

(3) Screeners must be able to hear and respond to the spoken voice and to audible alarms generated by screening equipment at an active screening location.

(4) Screeners who perform physical searches or other related operations must be able to efficiently and thoroughly manipulate and handle such baggage, containers, cargo, and other objects subject to screening.

(5) Screeners who perform pat-downs or hand-held metal detector searches of individuals must have sufficient dexterity and capability to thoroughly conduct those procedures over an individual's entire body.

(f) A screener must have the ability to read, speak, and write English well enough to—

(1) Carry out written and oral instructions regarding the proper performance of screening duties;

(2) Read English language identification media, credentials, airline tickets, documents, air waybills, invoices, and

labels on items normally encountered in the screening process;

(3) Provide direction to and understand and answer questions from English-speaking individuals undergoing screening; and

(4) Write incident reports and statements and log entries into security records in the English language.

(g) At locations outside the United States where the aircraft operator has operational control over a screening function, the aircraft operator may use screeners who do not meet the requirements of paragraph (f) of this section, provided that at least one representative of the aircraft operator who has the ability to functionally read and speak English is present while the aircraft operator's passengers are undergoing security screening. At such locations the aircraft operator may use screeners who are not United States citizens.

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, §1544.405 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1544.405 Qualifications of screening personnel.

§1544.407 New screeners: Training, testing, and knowledge of individuals who perform screening functions.

(a) *Training required.* Before performing screening functions, an individual must have completed initial, recurrent, and appropriate specialized training as specified in this section and the aircraft operator's security program. No aircraft operator may use any screener, screener in charge, or checkpoint security supervisor unless that individual has satisfactorily completed the required training. This paragraph does not prohibit the performance of screening functions during on-the-job training as provided in §1544.409 (b).

(b) *Use of training programs.* Training for screeners must be conducted under programs provided by TSA. Training programs for screeners-in-charge and checkpoint security supervisors must be conducted in accordance with the aircraft operator's security program.

(c) *Classroom instruction.* Each screener must complete at least 40 hours of classroom instruction or successfully complete a program that TSA determines will train individuals to a level of proficiency equivalent to the level that would be achieved by such classroom instruction.

(d) *Screener readiness test.* Before beginning on-the-job training, a screener trainee must pass the screener readiness test prescribed by TSA.

(e) *On-the-job training and testing.* Each screener must complete at least 60 hours of on-the-job training and must pass an on-the-job training test prescribed by TSA. No aircraft operator may permit a screener trainee to exercise independent judgment as a screener, until the individual passes an on-the-job training test prescribed by TSA.

(f) *Knowledge requirements.* Each aircraft operator must ensure that individuals performing as screeners, screeners-in-charge, and checkpoint security supervisors for the aircraft operator have knowledge of the provisions of this part, the aircraft operator's security program, and applicable Security Directives and Information Circulars to the extent necessary to perform their duties.

(g) *Disclosure of sensitive security information during training.* The aircraft operator may not permit a trainee to have access to sensitive security information during screener training unless a criminal history records check has successfully been completed for that individual in accordance with §1544.229, and the individual has no disqualifying criminal offense.

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, §1544.407 was amended by revising the section heading and paragraph (c), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1544.407 Training, testing, and knowledge of individuals who perform screening functions.

* * * * *

(c) *Citizenship.* A screener must be a citizen or national of the United States.

* * * * *

§ 1544.409 New screeners: Integrity of screener tests.

(a) *Cheating or other unauthorized conduct.* (1) Except as authorized by the TSA, no person may—

(i) Copy or intentionally remove a test under this part;

(ii) Give to another or receive from another any part or copy of that test;

(iii) Give help on that test to or receive help on that test from any person during the period that the test is being given; or

(iv) Use any material or aid during the period that the test is being given.

(2) No person may take any part of that test on behalf of another person.

(3) No person may cause, assist, or participate intentionally in any act prohibited by this paragraph (a).

(b) *Administering and monitoring screener tests.* (1) Each aircraft operator must notify TSA of the time and location at which it will administer each screener readiness test required under § 1544.405(d).

(2) Either TSA or the aircraft operator must administer and monitor the screener readiness test. Where more than one aircraft operator or foreign air carrier uses a screening location, TSA may authorize an employee of one or more of the aircraft operators or foreign air carriers to monitor the test for a trainee who will screen at that location.

(3) If TSA or a representative of TSA is not available to administer and monitor a screener readiness test, the aircraft operator must provide a direct employee to administer and monitor the screener readiness test.

(4) An aircraft operator employee who administers and monitors a screener readiness test must not be an instructor, screener, screener-in-charge, checkpoint security supervisor, or other screening supervisor. The employee must be familiar with the procedures for administering and monitoring the test and must be capable of observing whether the trainee or others are engaging in cheating or other unauthorized conduct.

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, § 1544.409 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1544.409 Integrity of screener tests.

§ 1544.411 New screeners: Continuing qualifications for screening personnel.

(a) *Impairment.* No individual may perform a screening function if he or she shows evidence of impairment, such as impairment due to illegal drugs, sleep deprivation, medication, or alcohol.

(b) *Training not complete.* An individual who has not completed the training required by § 1544.405 may be deployed during the on-the-job portion of training to perform security functions provided that the individual—

(1) Is closely supervised; and

(2) Does not make independent judgments as to whether individuals or property may enter a sterile area or aircraft without further inspection.

(c) *Failure of operational test.* No aircraft operator may use an individual to perform a screening function after that individual has failed an operational test related to that function, until that individual has successfully completed the remedial training specified in the aircraft operator's security program.

(d) *Annual proficiency review.* Each individual assigned screening duties shall receive an annual evaluation. The aircraft operator must ensure that a Ground Security Coordinator conducts and documents an annual evaluation of each individual who performs screening functions. An individual who performs screening functions may not continue to perform such functions unless the evaluation demonstrates that the individual—

(1) Continues to meet all qualifications and standards required to perform a screening function;

(2) Has a satisfactory record of performance and attention to duty based on the standards and requirements in the aircraft operator's security program; and

(3) Demonstrates the current knowledge and skills necessary to courteously, vigilantly, and effectively perform screening functions.

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, § 1544.411 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

PART 1546—FOREIGN AIR CARRIER SECURITY

Subpart A—General

Subpart B—Security Program

Subpart C—Operations

Subpart D—Threat and Threat Response

Subpart E—Screener Qualifications When the Foreign Air Carrier Conducts Screening

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44914, 44916–44917, 44935–44936, 44942, 46105.

SOURCE: 67 FR 8377, Feb. 22, 2002, unless otherwise noted.

Subpart A—General

§ 1546.1 Applicability of this part.

This part prescribes aviation security rules governing the following:

(a) The operation within the United States of each foreign air carrier holding a permit issued by the Department of Transportation under 49 U.S.C. 41302 or other appropriate authority issued by the former Civil Aeronautics Board or the Department of Transportation.

(b) Each law enforcement officer flying armed aboard an aircraft operated by a foreign air carrier described in paragraph (a) of this section.

§ 1546.3 TSA inspection authority.

(a) Each foreign air carrier must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with—

(1) This subchapter and any security program under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each foreign air carrier must provide evidence of compliance with this subchapter and its security program, including copies of records.

(c) TSA may enter and be present within secured areas, AOAs, SIDAs, and other areas where security measures required by TSA are carried out, without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

[67 FR 8377, Feb. 22, 2002, as amended at 71 FR 30511, May 26, 2006]

Subpart B—Security Program

§ 1546.101 Adoption and implementation.

Each foreign air carrier landing or taking off in the United States must adopt and carry out, for each scheduled and public charter passenger operation

or all-cargo operation, a security program that meets the requirements of—

(a) Section 1546.103(b) and subparts C, D, and E of this part for each operation with an aircraft having a passenger seating configuration of 61 or more seats;

(b) Section 1546.103(b) for each operation that will provide deplaned passengers access to a sterile area, or enplane passengers from a sterile area, when that access is not controlled by an aircraft operator using a security program under part 1544 of this chapter or a foreign air carrier using a security program under this part;

(c) Section 1546.103(b) for each operation with an airplane having a passenger seating configuration of 31 or more seats but 60 or fewer seats for which TSA has notified the foreign air carrier in writing that a threat exists; and

(d) Section 1546.103(c) for each operation with an airplane having a passenger seating configuration of 31 or more seats but 60 or fewer seats, when TSA has not notified the foreign air carrier in writing that a threat exists with respect to that operation.

(e) Sections 1546.103(b)(2) and (b)(4), 1546.202, 1546.205(a), (b), (c), (d), (e), and (f), 1546.207, 1546.211, 1546.213, and 1546.301 for each all-cargo operation with an aircraft having a maximum certificated take-off weight more than 45,500 kg (100,309.3 lbs.); and

(f) Sections 1546.103(b)(2) and (b)(4), 1546.202, 1546.205(a), (b), (d), and (f), 1546.211, and 1546.301 for each all-cargo operation with an aircraft having a maximum certificated take-off weight more than 12,500 pounds but not more than 45,500 kg (100,309.3 lbs.).

[67 FR 8377, Feb. 22, 2002, as amended at 71 FR 30511, May 26, 2006]

§ 1546.103 Form, content, and availability of security program.

(a) *General requirements.* The security program must be:

(1) *Acceptable to TSA.* A foreign air carrier's security program is acceptable only if TSA finds that the security program provides a level of protection similar to the level of protection provided by U.S. aircraft operators serving the same airports. Foreign air carriers must employ procedures equivalent to those required of U.S. aircraft operators serving the same airport, if TSA determines that such procedures are necessary to provide a similar level of protection.

(2) In English unless TSA requests that the program be submitted in the official language of the foreign air carrier's country.

(b) *Content of security program.* Each security program required by §1546.101(a), (b), (c), (e), or (f) must be designed to—

(1) Prevent or deter the carriage aboard airplanes of any unauthorized explosive, incendiary, or weapon on or about each individual's person or accessible property, except as provided in §1546.201(d), through screening by weapon-detecting procedures or facilities;

(2) Prohibit unauthorized access to airplanes;

(3) Ensure that checked baggage is accepted by a responsible agent of the foreign air carrier; and

(4) Prevent cargo and checked baggage from being loaded aboard its airplanes unless handled in accordance with the foreign air carrier's security procedures.

(c) *Law enforcement support.* Each security program required by §1546.101(d) must include the procedures used to comply with the applicable requirements of §1546.209 regarding law enforcement officers.

(d) *Availability.* Each foreign air carrier required to adopt and use a security program under this part must—

(1) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 1520 of this chapter, to persons with a need to know; and

(2) Refer requests for sensitive security information by other persons to TSA.

[67 FR 8377, Feb. 22, 2002, as amended at 71 FR 30512, May 26, 2006]

§ 1546.105 Acceptance of and amendments to the security program.

(a) *Initial acceptance of security program.* Unless otherwise authorized by TSA, each foreign air carrier required to have a security program by this part must submit its proposed program to

TSA at least 90 days before the intended date of passenger operations. TSA will notify the foreign air carrier of the security program's acceptability, or the need to modify the proposed security program for it to be acceptable under this part, within 30 days after receiving the proposed security program. The foreign air carrier may petition TSA to reconsider the notice to modify the security program within 30 days after receiving a notice to modify.

(b) *Amendment requested by a foreign air carrier.* A foreign air carrier may submit a request to TSA to amend its accepted security program as follows:

(1) The proposed amendment must be filed with the designated official at least 45 calendar days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the designated official.

(2) Within 30 calendar days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(3) An amendment to a foreign air carrier security program may be approved if the designated official determines that safety and the public interest will allow it, and the proposed amendment provides the level of security required under this part.

(4) Within 45 calendar days after receiving a denial, the foreign air carrier may petition the Administrator to reconsider the denial. A petition for reconsideration must be filed with the designated official.

(5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 calendar days of receipt by either directing the designated official to approve the amendment, or affirming the denial.

(6) Any foreign air carrier may submit a group proposal for an amendment that is on behalf of it and other aircraft operators that co-sign the proposal.

(c) *Amendment by TSA.* If the safety and the public interest require an amendment, the designated official may amend an accepted security program as follows:

(1) The designated official notifies the foreign air carrier, in writing, of the proposed amendment, fixing a period of not less than 45 calendar days within which the foreign air carrier may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the foreign air carrier of any amendment adopted or rescinds the notice. If the amendment is adopted, it becomes effective not less than 30 calendar days after the foreign air carrier receives the notice of amendment, unless the foreign air carrier petitions the Administrator to reconsider no later than 15 calendar days before the effective date of the amendment. The foreign air carrier must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 calendar days of receipt by either directing the designated official to withdraw or amend the amendment, or by affirming the amendment.

(d) *Emergency amendments.* If the designated official finds that there is an emergency requiring immediate action with respect to safety in air transportation or in air commerce that makes procedures in this section contrary to the public interest, the designated official may issue an amendment, without the prior notice and comment procedures in paragraph (c) of this section, effective without stay on the date the foreign air carrier receives notice of it. In such a case, the designated official will incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The foreign air carrier may file a petition for reconsideration under paragraph (c) of this section; however, this does not

stay the effectiveness of the emergency amendment.

Subpart C—Operations

§ 1546.201 Acceptance and screening of individuals and accessible property.

(a) *Preventing or deterring the carriage of any explosive, incendiary, or weapon.* Unless otherwise authorized by TSA, each foreign air carrier must use the measures in its security program to prevent or deter the carriage of any explosive, incendiary, or weapon on or about each individual's person or accessible property before boarding an aircraft or entering a sterile area.

(b) *Screening of individuals and accessible property.* Except as provided in its security program, each foreign air carrier must ensure that each individual entering a sterile area at each preboard screening checkpoint for which it is responsible, and all accessible property under that individual's control, are inspected for weapons, explosives, and incendiaries as provided in § 1546.207.

(c) *Refusal to transport.* Each foreign air carrier conducting an operation for which a security program is required by § 1546.101(a), (b), or (c) must refuse to transport—

(1) Any individual who does not consent to a search or inspection of his or her person in accordance with the system prescribed in this part; and

(2) Any property of any individual or other person who does not consent to a search or inspection of that property in accordance with the system prescribed by this part.

(d) *Explosive, incendiary, weapon: Prohibitions and exceptions.* No individual may, while on board an aircraft being operated by a foreign air carrier in the United States, carry on or about his person a deadly or dangerous weapon, either concealed or unconcealed. This paragraph (d) does not apply to—

(1) Officials or employees of the state of registry of the aircraft who are authorized by that state to carry arms; and

(2) Crewmembers and other individuals authorized by the foreign air carrier to carry arms.

§ 1546.202 Persons and property onboard the aircraft.

Each foreign air carrier operating under § 1546.101(e) or (f) must apply the security measures in its security program for persons who board the aircraft for transportation, and for their property, to prevent or deter the carriage of any unauthorized persons, and any unauthorized weapons, explosives, incendiaries, and other destructive devices, items, or substances.

[71 FR 30512, May, 26, 2006]

§ 1546.203 Acceptance and screening of checked baggage.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each foreign air carrier must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized explosive or incendiary onboard aircraft in checked baggage.

(b) *Refusal to transport.* Each foreign air carrier must refuse to transport any individual's checked baggage or property if the individual does not consent to a search or inspection of that checked baggage or property in accordance with the system prescribed by this part.

(c) *Firearms in checked baggage.* No foreign air carrier may knowingly permit any person to transport, nor may any person transport, while aboard an aircraft being operated in the United States by that carrier, in checked baggage, a firearm, unless:

(1) The person has notified the foreign air carrier before checking the baggage that the firearm is in the baggage; and

(2) The baggage is carried in an area inaccessible to passengers.

§ 1546.205 Acceptance and screening of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each foreign air carrier operating a program under § 1546.101(a), (b), (e), or (f) must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized person, and

any unauthorized explosive, incendiary, and other destructive substance or item in cargo onboard an aircraft.

(b) *Refusal to transport.* Each foreign air carrier operating a program under §1546.101(a), (b), (e), or (f) must refuse to transport any cargo, if the shipper does not consent to a search or inspection of that cargo in accordance with the system prescribed by this part.

(c) *Control.* Each foreign air carrier operating a program under §1546.101(a), (b), or (e) must use the procedures in its security program to control cargo that it accepts for transport on an aircraft in a manner that—

(1) Prevents the carriage of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item onboard the aircraft.

(2) Prevents access by unauthorized persons other than an authorized foreign air carrier employee or agent, or persons authorized by the airport operator or host government.

(d) *Screening and inspection of cargo in the United States.* Each foreign air carrier operating a program under §1546.101(a), (b), (e), or (f) must ensure that, as required in its security program, cargo is screened and inspected for any unauthorized persons, and any unauthorized explosives, incendiaries, and other destructive substances or items as provided in the foreign air carrier's security program, and §1546.207, and as provided in §1546.213 for operations under §1546.101(a) or (b) before loading it on its aircraft in the United States.

(e) *Acceptance of cargo in the United States only from specified persons.* Each foreign air carrier operating a program under §1546.101(a), (b), or (e) of this part may accept cargo in the United States only from the shipper, or from an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program as provided in its security program.

(f) *Acceptance of cargo to be loaded for transport to the United States.* Each foreign air carrier subject to this part that accepts cargo to be loaded on its aircraft for transport to the United States must carry out the requirements of its security program.

[71 FR 30512, May 26, 2006]

EFFECTIVE DATE NOTE: At 74 FR 47704, Sept. 16, 2009, §1546.205 was amended by revising paragraphs (d), (e) and adding a new (g), effective November 16, 2009. For the convenience of the user, the added and revised text is set forth as follows:

§ 1546.205 Acceptance and screening of cargo.

* * * * *

(d) *Screening and inspection of cargo in the United States.* For cargo to be loaded in the United States, each foreign air carrier operating a program under §1546.101(1)(a), (b), (e), or (f) must ensure that cargo is screened and inspected for any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substances or items as provided in the foreign air carrier's security program and §1546.207, and as provided in §1546.213 for operations under §1546.101(a) or (b), before loading it on its aircraft in the United States.

(e) *Acceptance of cargo only from specified persons.* Except as otherwise provided in its program, each foreign air carrier operating a program under §1546.101(a), (b), (e) or (f) may accept cargo for air transportation to be loaded in the United States only from the shipper, or from an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program, or, in the case of a foreign air carrier under §1546.101(a) or (b), from a certified cargo screening facility, as provided in its security program.

* * * * *

(g) *Screening of cargo loaded inside the United States under §1546.101(a) or (b).* For cargo to be loaded in the United States, each foreign air carrier under §1546.101(a) or (b) must ensure that all cargo is screened in the United States as follows:

(1) *Amount screened.* (i) Not later than February 3, 2009, each foreign air carrier must ensure that at least 50 percent of its cargo is screened prior to transport on a passenger aircraft.

(ii) Not later than August 3, 2010, each foreign air carrier must ensure that 100 percent of its cargo is screened prior to transport on a passenger aircraft.

(2) *Methods of screening.* For the purposes of this paragraph (g), the foreign air carrier must ensure that cargo is screened using a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security, as provided in its

security program. Such methods may include TSA-approved x-ray systems, explosives detection systems, explosives trace detection, explosives detection canine teams certified by TSA, a physical search together with manifest verification, or other method approved by TSA.

(3) *Limitation on who may conduct screening.* Screening must be conducted by the foreign air carrier on an airport, by another aircraft operator or foreign air carrier operating under a security program under this chapter with a comparable cargo security program on an airport with a complete program under 49 CFR part 1542, by a certified cargo screening facility in accordance with 49 CFR part 1549, or by TSA. If an aircraft operator or foreign air carrier screens cargo off an airport, it must do so as a certified cargo screening facility in accordance with part 1549.

(4) The foreign air carrier must verify that the chain of custody measures for the screened cargo are intact prior to loading such cargo on aircraft, or must ensure that the cargo is re-screened in accordance with this chapter.

§ 1546.207 Screening of individuals and property.

(a) *Applicability of this section.* This section applies to the inspection of individuals, accessible property, checked baggage, and cargo as required under this part.

(b) *Locations within the United States at which TSA conducts screening.* As required in its security program, each foreign air carrier must ensure that all individuals or property have been inspected by TSA before boarding or loading on its aircraft. This paragraph applies when TSA is conducting screening using TSA employees or when using companies under contract with TSA.

(c) *Foreign air carrier conducting screening.* Each foreign air carrier must use the measures in its security program to inspect the individual or property. This paragraph does not apply at locations identified in paragraphs (b) of this section.

§ 1546.209 Use of X-ray systems.

(a) *TSA authorization required.* No foreign air carrier may use any X-ray system within the United States to screen accessible property or checked baggage, unless specifically authorized under its security program. No foreign air carrier may use such a system in a manner contrary to its security program. TSA authorizes foreign air carriers to use X-ray systems for inspecting accessible property or checked baggage under a security program if the foreign air carrier shows that—

(1) The system meets the standards for cabinet X-ray systems primarily for the inspection of baggage issued by the Food and Drug Administration (FDA) and published in 21 CFR 1020.40;

(2) A program for initial and recurrent training of operators of the system is established, which includes training in radiation safety, the efficient use of X-ray systems, and the identification of weapons, explosives, and incendiaries; and

(3) The system meets the imaging requirements set forth in its security program using the step wedge specified in American Society for Testing Materials (ASTM) Standard F792–88 (Reapproved 1993). This standard is incorporated by reference in paragraph (g) of this section.

(b) *Annual radiation survey.* No foreign air carrier may use any X-ray system unless, within the preceding 12 calendar months, a radiation survey is conducted that shows that the system meets the applicable performance standards in 21 CFR 1020.40.

(c) *Radiation survey after installation or moving.* No foreign air carrier may use any X-ray system after the system has been installed at a screening point or after the system has been moved unless a radiation survey is conducted which shows that the system meets the applicable performance standards in 21 CFR 1020.40. A radiation survey is not required for an X-ray system that is designed and constructed as a mobile unit and the foreign air carrier shows that it can be moved without altering its performance.

(d) *Defect notice or modification order.* No foreign air carrier may use any X-ray system that is not in full compliance with any defect notice or modification order issued for that system by the FDA, unless the FDA has advised TSA that the defect or failure to comply does not create a significant risk of injury, including genetic injury, to any person.

(e) *Signs and inspection of photographic equipment and film.* (1) At locations at which a foreign air carrier uses an X-ray system to inspect accessible property the foreign air carrier must ensure that a sign is posted in a conspicuous place at the screening checkpoint.

(2) At locations at which a foreign air carrier or TSA uses an X-ray system to inspect checked baggage the foreign air carrier must ensure that a sign is posted in a conspicuous place where the foreign air carrier accepts checked baggage.

(3) The signs required under this paragraph must notify individuals that such items are being inspected by an X-ray and advise them to remove all X-ray, scientific, and high-speed film from accessible property and checked baggage before inspection. This sign must also advise individuals that they may request that an inspection be made of their photographic equipment and film packages without exposure to an X-ray system. If the X-ray system exposes any accessible property or checked baggage to more than one milliroentgen during the inspection, the sign must advise individuals to remove film of all kinds from their articles before inspection.

(4) If requested by individuals, their photographic equipment and film packages must be inspected without exposure to an X-ray system.

(f) *Radiation survey verification after installation or moving.* Each foreign air carrier must maintain at least one copy of the results of the most recent radiation survey conducted under paragraph (b) or (c) of this section and must make it available for inspection upon request by TSA at each of the following locations—

(1) The foreign air carrier's principal business office; and

(2) The place where the X-ray system is in operation.

(g) *Incorporation by reference.* The American Society for Testing and Materials (ASTM) Standard F792–88 (Reapproved 1993), ''Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas,'' is approved for incorporation by reference by the Director of the Federal Register pursuant to 5 U.S.C. 552(a) and 1 CFR part 51. ASTM Standard F792–88 may be examined at the Department of Transportation (DOT) Docket, 400 Seventh Street SW, Room Plaza 401, Washington, DC 20590, or on DOT's Docket Management System (DMS) web page at *http://dms.dot.gov/search* (under docket number FAA–2001–8725). Copies of the standard may be examined also at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741–6030, or go to: *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html.* In addition, ASTM Standard F792–88 (Reapproved 1993) may be obtained from the American Society for Testing and Materials, 100 Barr Harbor Drive, West Conshohocken, PA 19428–2959.

(h) Each foreign air carrier must comply with the X-ray operator duty time limitations specified in its security program.

[67 FR 8377, Feb. 22, 2002, as amended at 69 FR 18803, Apr. 9, 2004]

§ 1546.211 Law enforcement personnel.

(a) At airports within the United States not governed by part 1542 of this chapter, each foreign air carrier engaging in public charter passenger operations must—

(1) When using a screening system required by §1546.101(a), (b), or (c), provide for law enforcement officers meeting the qualifications and standards, and in the number and manner, specified in part 1542; and

(2) When using an airplane having a passenger seating configuration of 31 or more but 60 or fewer seats for which a screening system is not required by §1546.101(a), (b), or (c), arrange for law enforcement officers meeting the qualifications and standards specified in part 1542 of this chapter to be available to respond to an incident and provide to appropriate employees, including crewmembers, current information with respect to procedures for obtaining law enforcement assistance at that airport.

(b) At airports governed by part 1542 of this chapter, each foreign air carrier

engaging in scheduled passenger operations or public charter passenger operations when using an airplane with a passenger seating configuration of 31 or more and 60 or fewer seats under §1546.101(c), must arrange for law enforcement personnel meeting the qualifications and standards specified in part 1542 of this chapter to be available to respond to an incident and provide to appropriate employees, including crewmembers, current information with respect to procedures for obtaining law enforcement assistance at that airport.

§1546.213 Access to cargo: Security threat assessments for cargo personnel in the United States.

This section applies in the United States to each foreign air carrier operating under §1546.101(a), (b), or (e).

(a) This section applies to each employee or agent in the United States whom the foreign air carrier authorizes to have unescorted access to cargo from the time—

(1) The cargo reaches a location where a foreign air carrier operating under §1546.101(e) consolidates or inspects it pursuant to security program requirements, until the cargo enters an airport Security Identification Display Area or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier, or

(2) A foreign air carrier under §1546.101(a) or (b) accepts the cargo, until the cargo—

(i) Enters an airport Security Identification Display Area;

(ii) Is removed from the destination airport; or

(iii) Is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier.

(b) Before a foreign air carrier authorizes, and before an employee or agent gains, unescorted access to cargo as described in paragraph (a) of this section, each employee or agent must successfully complete one of the following:

(1) A criminal history records check under §1542.209, §1544.229, or §1544.230 of this chapter, if the employee or agent is otherwise required to undergo that check.

(2) A Security Threat Assessment under part 1540 subpart C of this chapter. An employee or agent who has successfully completed this Security Threat Assessment for one employer need not complete it for another employer, if the employee or agent has been continuously employed in a position that requires a Security Threat Assessment.

(3) Another Security Threat Assessment approved by TSA as comparable to paragraphs (b)(1) or (2) of this section.

(c) Each foreign air carrier must ensure that each individual who has access to its cargo—

(1) Has successfully completed one of the checks in paragraph (b) of this section;

(2) Is escorted by an employee or agent who has successfully completed one of the checks in paragraph (b) of this section; or

(3) Is authorized to serve as law enforcement personnel at that location.

(d) Operators must submit to TSA the names and other identifying information required by TSA of all individuals required to successfully complete an assessment under paragraph (b) not later than May 15, 2007, for direct employees and not later than July 15, 2007, for agents. After those dates, the operators may not allow an individual to perform a function for which a STA is required, unless the operator has submitted the information for that individual to TSA.

(e) Operators must comply with the requirements of paragraphs (a), (b), and (c) of this section not later than the dates to be specified by TSA in a future rule in the FEDERAL REGISTER.

[71 FR 30512, May 26, 2006; 71 FR 31964, June 2, 2006, as amended at 71 FR 62549, Oct. 25, 2006; 72 FR 13026, Mar. 20, 2007]

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1546.213 was revised, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1546.213 Access to cargo: Security threat assessments for cargo personnel in the United States.

This section applies in the United States to each foreign air carrier operating under §1546.101(a), (b), or (e).

(a) Before a foreign air carrier authorizes and before an individual performs a function described in paragraph (b) of this section—

(1) Each individual must successfully complete a security threat assessment or comparable security threat assessment described in part 1540 subpart C of this chapter; and

(2) Each aircraft operator must complete the requirements in part 1540 subpart C.

(b) The security threat assessment required in paragraph (a) of this section applies to the following:

(1) Each individual who has unescorted access to cargo and access to information that such cargo will be transported on a passenger aircraft; or who has unescorted access to cargo that has been screened for transport on a passenger aircraft; or who performs certain functions related to the transportation, dispatch or security of cargo for transport on a passenger aircraft or all-cargo aircraft, as specified in the foreign air craft operator's or foreign air carrier's security program; from the time—

(i) The cargo reaches a location where a foreign air carrier operating under §1546.101(e) consolidates or inspects it pursuant to security program requirements, until the cargo enters an airport Security Identification Display Area or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier; or

(ii) A foreign air carrier under §§1546.101(a) or (b) accepts the cargo, until the cargo—

(A) Enters an airport Security Identification Display Area;

(B) Is removed from the destination airport; or

(C) Is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier.

(2) Each individual the foreign air carrier authorizes to screen cargo or to supervise the screening of cargo under §1546.205.

§1546.215 Known shipper program.

This section applies to each foreign air carrier operating a program under §1546.101(a) or (b).

(a) For cargo to be loaded on its aircraft in the United States, each foreign air carrier must have and carry out a known shipper program in accordance with its security program. The program must—

(1) Determine the shipper's validity and integrity as provided in the foreign air carrier's security program;

(2) Provide that the foreign air carrier will separate known shipper cargo from unknown shipper cargo; and

(3) Provide for the foreign air carrier to ensure that cargo is screened or inspected as set forth in its security program.

(b) When required by TSA, each foreign air carrier must submit in a form and manner acceptable to TSA—

(1) Information identified in its security program regarding an applicant to be a known shipper or a known shipper; and

(2) Corrections and updates to the information upon learning of a change to the information specified in paragraph (b)(1) of this section.

[71 FR 30512, May 26, 2006]

Subpart D—Threat and Threat Response

§1546.301 Bomb or air piracy threats.

No foreign air carrier may land or take off an airplane in the United States after receiving a bomb or air piracy threat against that airplane, unless the following actions are taken:

(a) If the airplane is on the ground when a bomb threat is received and the next scheduled flight of the threatened airplane is to or from a place in the United States, the foreign air carrier ensures that the pilot in command is advised to submit the airplane immediately for a security inspection and an inspection of the airplane is conducted before the next flight.

(b) If the airplane is in flight to a place in the United States when a bomb threat is received, the foreign air carrier ensures that the pilot in command is advised immediately to take the emergency action necessary under the circumstances and a security inspection of the airplane is conducted immediately after the next landing.

(c) If information is received of a bomb or air piracy threat against an airplane engaged in an operation specified in paragraph (a) or (b) of this section, the foreign air carrier ensures that notification of the threat is given to the appropriate authorities of the State in whose territory the airplane is located or, if in flight, the appropriate authorities of the State in whose territory the airplane is to land.

[67 FR 8377, Feb. 22, 2002, as amended at 71 FR 30513, May 26, 2006]

Subpart E—Screener Qualifications When the Foreign Air Carrier Conducts Screening

§ 1546.401 Applicability of this subpart.

(a) *Foreign air carrier screening.* This subpart applies when the foreign air carrier is conducting inspections as provided in § 1546.207(c).

(b) *Current screeners.* As used in this subpart, ''current screener'' means each individual who first performed screening functions before the date the foreign air carrier must begin use of the new screener training program provided by TSA. Until November 19, 2002, each current screener must comply with § 1546.403. Until November 19, 2002, each foreign air carrier must apply § 1546.403 for each current screener. On and after November 19, 2002, each current screener must comply with §§ 1546.405 through 1546.411, and each foreign air carrier must comply with §§ 1546.405 through 1546.411 for such individuals.

(c) *New screeners.* As used in this subpart, ''new screener'' means each individual who first performs screening functions on and after TSA orders the foreign air carrier to begin use of the new screener training program provided by TSA. Each foreign air carrier must apply §§ 1546.405 through 1546.411 for new screeners.

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, § 1546.401 was revised, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1546.401 Applicability of this subpart.

This subpart applies when the aircraft operator is conducting inspections as provided in § 1546.207.

§ 1546.403 Current screeners.

The foreign air carrier must ensure that each current screener it uses to perform screening functions meet the qualifications and training standards set forth in its security program. This section is no longer effective on and after November 19, 2002.

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, § 1546.403 was removed and reserved, effective November 16, 2009.

§ 1546.405 New screeners: Qualifications of screening personnel.

(a) No individual subject to this subpart may perform a screening function unless that individual has the qualifications described in §§ 1546.405 through 1546.411. No foreign air carrier may use such an individual to perform a screening function unless that person complies with the requirements of §§ 1546.405 through 1546.411.

(b) A screener must have a satisfactory or better score on a screener selection test administered by TSA.

(c) A screener must be a citizen of the United States.

(d) A screener must have a high school diploma, a General Equivalency Diploma, or a combination of education and experience that TSA has determined to be sufficient for the individual to perform the duties of the position.

(e) A screener must have basic aptitudes and physical abilities including color perception, visual and aural acuity, physical coordination, and motor skills to the following standards:

(1) Screeners operating screening equipment must be able to distinguish on the screening equipment monitor the appropriate imaging standard specified in the foreign air carrier's security program.

(2) Screeners operating any screening equipment must be able to distinguish each color displayed on every type of screening equipment and explain what each color signifies.

(3) Screeners must be able to hear and respond to the spoken voice and to audible alarms generated by screening equipment at an active screening location.

(4) Screeners who perform physical searches or other related operations must be able to efficiently and thoroughly manipulate and handle such baggage, containers, cargo, and other objects subject to screening.

(5) Screeners who perform pat-downs or hand-held metal detector searches of individuals must have sufficient dexterity and capability to thoroughly conduct those procedures over an individual's entire body.

(f) A screener must have the ability to read, speak, and write English well enough to—

(1) Carry out written and oral instructions regarding the proper performance of screening duties;

(2) Read English language identification media, credentials, airline tickets, documents, air waybills, invoices, and labels on items normally encountered in the screening process;

(3) Provide direction to and understand and answer questions from English-speaking individuals undergoing screening; and

(4) Write incident reports and statements and log entries into security records in the English language.

(g) At locations outside the United States that are the last point of departure to the United States, and where the foreign air carrier has operational control over a screening function, the foreign air carrier may use screeners who do not meet the requirements of paragraph (f) of this section. At such locations the foreign air carrier may use screeners who are not United States citizens.

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1546.405 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1546.405 Qualifications of screening personnel.

§1546.407 New screeners: Training, testing, and knowledge of individuals who perform screening functions.

(a) *Training required.* Before performing screening functions, an individual must have completed initial, recurrent, and appropriate specialized training as specified in this section and the foreign air carrier's security program. No foreign air carrier may use any screener, screener in charge, or checkpoint security supervisor unless that individual has satisfactorily completed the required training. This paragraph does not prohibit the performance of screening functions during on-the-job training as provided in §1544.409(b).

(b) *Use of training programs.* Training for screeners must be conducted under programs provided by TSA. Training programs for screeners-in-charge and checkpoint security supervisors must be conducted in accordance with the foreign air carrier's security program.

(c) *Classroom instruction.* Each screener must complete at least 40 hours of classroom instruction or successfully complete a program that TSA determines will train individuals to a level of proficiency equivalent to the level that would be achieved by such classroom instruction.

(d) *Screener readiness test.* Before beginning on-the-job training, a screener trainee must pass the screener readiness test prescribed by TSA.

(e) *On-the-job training and testing.* Each screener must complete at least 60 hours of on-the-job training and must pass an on-the-job training test prescribed by TSA. No foreign air carrier may permit a screener trainee to exercise independent judgment as a screener, until the individual passes an on-the-job training test prescribed by TSA.

(f) *Knowledge requirements.* Each foreign air carrier must ensure that individuals performing as screeners, screeners-in-charge, and checkpoint security supervisors for the foreign air carrier have knowledge of the provisions of this part, the foreign air carrier's security program, and applicable emergency amendments to the foreign air carrier's security program to the extent necessary to perform their duties.

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1546.407 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1546.407 Training, testing, and knowledge of individuals who perform screening functions.

§1546.409 New screeners: Integrity of screener tests.

(a) *Cheating or other unauthorized conduct.* (1) Except as authorized by TSA, no person may—

(i) Copy or intentionally remove a test under this part;

(ii) Give to another or receive from another any part or copy of that test;

(iii) Give help on that test to or receive help on that test from any person during the period that the test is being given; or

(iv) Use any material or aid during the period that the test is being given.

(2) No person may take any part of that test on behalf of another person.

(3) No person may cause, assist, or participate intentionally in any act prohibited by this paragraph (a).

(b) *Administering and monitoring screener tests.* (1) Each foreign air carrier must notify TSA of the time and location at which it will administer each screener readiness test required under §1544.405 (d).

(2) Either TSA or the foreign air carrier must administer and monitor the screener readiness test. Where more than one foreign air carrier or foreign air carrier uses a screening location, TSA may authorize an employee of one or more of the foreign air carriers or foreign air carriers to monitor the test for a trainee who will screen at that location.

(3) If TSA or a representative of TSA is not available to administer and monitor a screener readiness test, the foreign air carrier must provide a direct employee to administer and monitor the screener readiness test.

(4) An foreign air carrier employee who administers and monitors a screener readiness test must not be an instructor, screener, screener-in-charge, checkpoint security supervisor, or other screening supervisor. The employee must be familiar with the procedures for administering and monitoring the test and must be capable of observing whether the trainee or others are engaging in cheating or other unauthorized conduct.

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1546.409 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1546.409 Integrity of screener tests.

§1546.411 New screeners: Continuing qualifications for screening personnel.

(a) *Impairment.* No individual may perform a screening function if he or she shows evidence of impairment, such as impairment due to illegal drugs, sleep deprivation, medication, or alcohol.

(b) *Training not complete.* An individual who has not completed the training required by §1546.405 may be deployed during the on-the-job portion of training to perform security functions provided that the individual—

(1) Is closely supervised; and

(2) Does not make independent judgments as to whether individuals or property may enter a sterile area or aircraft without further inspection.

(c) *Failure of operational test.* No foreign air carrier may use an individual to perform a screening function after that individual has failed an operational test related to that function, until that individual has successfully completed the remedial training specified in the foreign air carrier's security program.

(d) *Annual proficiency review.* Each individual assigned screening duties shall receive an annual evaluation. The foreign air carrier must conduct and document an annual evaluation of each individual who performs screening functions. An individual who performs screening functions may not continue to perform such functions unless the evaluation demonstrates that the individual—

(1) Continues to meet all qualifications and standards required to perform a screening function;

(2) Has a satisfactory record of performance and attention to duty based on the standards and requirements in the foreign air carrier's security program; and

(3) Demonstrates the current knowledge and skills necessary to courteously, vigilantly, and effectively perform screening functions.

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1546.411 was amended by revising the section heading, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1546.411 Continuing qualifications of screening personnel.

PART 1548—INDIRECT AIR CARRIER SECURITY

Sec.

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44913–44914, 44916–44917, 44932, 44935–44936, 46105.

SOURCE: 67 FR 8382, Feb. 22, 2002, unless otherwise noted.

§ 1548.1 Applicability of this part.

This part prescribes aviation security rules governing each indirect air carrier engaged indirectly in the air transportation of property on aircraft.

[67 FR 8382, Feb. 22, 2002, as amended at 71 FR 33255, June 8, 2006]

§ 1548.3 TSA inspection authority.

(a) Each indirect air carrier must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or airport tenant with—

(1) This subchapter, and any security program approved under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each indirect air carrier must provide evidence of compliance with this subchapter and its indirect air carrier security program, including copies of records.

(c) TSA may enter and be present within areas where security measures required by TSA are carried out without access media or identification media issued or approved by the indirect air carrier, an airport operator, or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

[67 FR 8382, Feb. 22, 2002, as amended at 71 FR 30513, May 26, 2006]

§ 1548.5 Adoption and implementation of the security program.

(a) *Security program required.* No indirect air carrier may offer cargo to an aircraft operator operating under a full program or a full all-cargo program specified in part 1544 of this subchapter, or to a foreign air carrier operating under a program under §1546.101(a), (b), or (e) of this subchapter, unless that indirect air carrier has and carries out an approved security program under this part. Each indirect air carrier that does not currently hold a security program under part 1548, and that offers cargo to an aircraft operator operating under a full all-cargo program or a comparable operation by a foreign air carrier must comply with this section not later than December 1, 2006.

(b) *General requirements.* (1) The security program must provide for the security of the aircraft, as well as that of persons and property traveling in air transportation against acts of criminal violence and air piracy and against the introduction into the aircraft of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item as provided in the indirect air carrier's security program. This requirement applies—

(i) From the time the indirect air carrier accepts the cargo to the time it transfers the cargo to an entity that is not an employee or agent of the indirect air carrier;

(ii) While the cargo is stored, en route, or otherwise being handled by an employee or agent of the indirect air carrier; and

(iii) Regardless of whether the indirect air carrier has or ever had physical possession of the cargo.

(2) The indirect air carrier must ensure that its employees and agents carry out the requirements of this chapter and the indirect air carrier's security program.

(c) *Content.* Each security program under this part must—

(1) Be designed to prevent or deter the introduction of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item onto an aircraft.

(2) Include the procedures and description of the facilities and equipment used to comply with the requirements of §§ 1548.9 and 1548.17 regarding the acceptance and offering of cargo.

(3) Include the procedures and syllabi used to accomplish the training required under § 1548.11 of persons who accept, handle, transport, or deliver cargo on behalf of the indirect air carrier.

(d) *Availability*. Each indirect air carrier having a security program must:

(1) Maintain an original of the security program at its corporate office.

(2) Have accessible a complete copy, or the pertinent portions of its security program, or appropriate implementing instructions, at each office where cargo is accepted. An electronic version is adequate.

(3) Make a copy of the security program available for inspection upon the request of TSA.

(4) Restrict the distribution, disclosure, and availability of information contained in its security program to persons with a need to know, as described in part 1520 of this chapter.

(5) Refer requests for such information by other persons to TSA.

[67 FR 8382, Feb. 22, 2002, as amended at 71 FR 30513, May 26, 2006; 71 FR 31964, June 2, 2006]

§ 1548.7 Approval, amendment, annual renewal, and withdrawal of approval of the security program.

(a) *Original Application*—(1) *Application*. The applicant must apply for a security program in a form and a manner prescribed by TSA not less than 90 calendar days before the applicant intends to begin operations. The application must be in writing and include:

(i) The business name; other names, including doing business as; state of incorporation, if applicable; and tax identification number.

(ii) The applicant names, addresses, and dates of birth of each proprietor, general partner, officer, director, and owner identified under § 1548.16.

(iii) A signed statement from each person listed in paragraph (a)(1)(ii) of this section stating whether he or she has been a proprietor, general partner, officer, director, or owner of an IAC that had its security program withdrawn by TSA.

(iv) Copies of government-issued identification of persons listed in paragraph (a)(1)(ii) of this section.

(v) Addresses of all business locations in the United States.

(vi) A statement declaring whether the business is a '''small business''' pursuant to section 3 of the Small Business Act (15 U.S.C. 632).

(vii) A statement acknowledging and ensuring that each employee and agent of the indirect air carrier, who is subject to training under § 1548.11, will have successfully completed the training outlined in its security program before performing security-related duties.

(viii) Other information requested by TSA concerning Security Threat Assessments.

(ix) A statement acknowledging and ensuring that each employee and agent will successfully complete a Security Threat Assessment under § 1548.15 before authorizing the individual to have unescorted access to cargo.

(2) *Approval*. TSA will approve the security program by providing the indirect air carrier with the Indirect Air Carrier Standard Security Program and any Security Directive upon determining that—

(i) The indirect air carrier has met the requirements of this part, its security program, and any applicable Security Directive;

(ii) The approval of its security program is not contrary to the interests of security and the public interest; and

(iii) The indirect air carrier has not held a security program that was withdrawn within the previous year, unless otherwise authorized by TSA.

(3) *Commencement of operations*. The indirect air carrier may operate under a security program when it meets all requirements, including but not limited to successful completion of training and Security Threat Assessments by relevant personnel.

(4) *Duration of security program*. The security program will remain effective

until the end of the calendar month one year after the month it was approved.

(5) *Requirement to report changes in information.* Each indirect air carrier with an approved security program under this part must notify TSA, in a form and manner approved by TSA, of any changes to the information submitted during its initial application.

(i) This notification must be submitted to the designated official not later than 30 days after the date the change occurred.

(ii) Changes included in the requirement of this paragraph include, but are not limited to, changes in the indirect air carrier's contact information, owners, business addresses and locations, and form of business entity.

(b) *Renewal Application.* Upon timely submittal of an application for renewal, and unless and until TSA denies the application, the indirect air carrier's approved security program remains in effect.

(1) Unless otherwise authorized by TSA, each indirect air carrier that has a security program under this part must timely submit to TSA, at least 30 calendar days prior to the first day of the anniversary month of initial approval of its security program, an application for renewal of its security program in a form and a manner approved by TSA.

(2) The application for renewal must be in writing and include a signed statement that the indirect air carrier has reviewed and ensures the continuing accuracy of the contents of its initial application for a security program, subsequent renewal applications, or other submissions to TSA confirming a change of information and noting the date such applications and submissions were sent to TSA, including the following certification:

[Name of indirect air carrier] (hereinafter ''the IAC'') has adopted and is currently carrying out a security program in accordance with the Transportation Security Regulations as originally approved on [Insert date of TSA initial approval]. In accordance with TSA regulations, the IAC has notified TSA of any new or changed information required for the IAC's initial security program. If new or changed information is being submitted to TSA as part of this application for renewal, that information is stated in this filing.

The IAC understands that intentional falsification of certification to an air carrier or to TSA may be subject to both civil and criminal penalties under 49 CFR 1540 and 1548 and 18 U.S.C. 1001. Failure to notify TSA of any new or changed information required for initial approval of the IAC's security program in a timely fashion and in a form acceptable to TSA may result in withdrawal by TSA of approval of the IAC's security program.

(3) TSA will renew approval of the security program if TSA determines that—

(i) The indirect air carrier has met the requirements of this chapter, its security program, and any Security Directive; and

(ii) The renewal of its security program is not contrary to the interests of security and the public interest.

(4) If TSA determines that the indirect air carrier meets the requirements of paragraph (b)(3) of this section, it will renew the indirect air carrier's security program. The security program will remain effective until the end of the calendar month one year after the month it was renewed.

(c) *Amendment requested by an indirect air carrier or applicant.* An indirect air carrier or applicant may file a request for an amendment to its security program with the TSA designated official at least 45 calendar days before the date it proposes for the amendment to become effective, unless the designated official allows a shorter period. Any indirect air carrier may submit a group proposal for an amendment that is on behalf of it and other indirect air carriers that co-sign the proposal.

(1) Within 30 calendar days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(2) An amendment to an indirect air carrier security program may be approved, if the designated official determines that safety and the public interest will allow it, and if the proposed amendment provides the level of security required under this part.

(3) Within 30 calendar days after receiving a denial of the proposed amendment, the indirect air carrier may petition TSA to reconsider the denial. A

petition for reconsideration must be filed with the designated official.

(4) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to the TSA for reconsideration. TSA will dispose of the petition within 30 calendar days of receipt by either directing the designated official to approve the amendment or by affirming the denial.

(d) *Amendment by TSA.* TSA may amend a security program in the interest of safety and the public interest, as follows:

(1) TSA notifies the indirect air carrier, in writing, of the proposed amendment, fixing a period of not less than 30 calendar days within which the indirect air carrier may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the indirect air carrier of any amendment adopted or rescinds the notice of amendment. If the amendment is adopted, it becomes effective not less than 30 calendar days after the indirect air carrier receives the notice of amendment, unless the indirect air carrier disagrees with the proposed amendment and petitions the TSA to reconsider, no later than 15 calendar days before the effective date of the amendment. The indirect air carrier must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice of amendment, or transmits the petition, together with any pertinent information, to TSA for reconsideration. TSA disposes of the petition within 30 calendar days of receipt, either by directing the designated official to withdraw or amend the notice of amendment, or by affirming the notice of amendment.

(e) *Emergency Amendments.* (1) If TSA finds that there is an emergency requiring immediate action, with respect to aviation security that makes procedures in this section contrary to the public interest, the designated official may issue an emergency amendment, without the prior notice and comment procedures described in paragraph (d) of this section.

(2) The emergency amendment is effective without stay on the date the indirect air carrier receives notification. TSA will incorporate in the notification a brief statement of the reasons and findings for the emergency amendment to be adopted.

(3) The indirect air carrier may file a petition for reconsideration with the TSA no later than 15 calendar days after TSA issued the emergency amendment. The indirect air carrier must send the petition for reconsideration to the designated official; however, the filing does not stay the effective date of the emergency amendment.

(f) *Withdrawal of approval of a security program.* TSA may withdraw the approval of the indirect air carrier's security program, if TSA determines continued operation is contrary to safety and the public interest, as follows:

(1) *Notice of proposed withdrawal of approval.* The designated official will serve a notice of proposed withdrawal of approval, which notifies the indirect air carrier, in writing, of the facts, charges, and applicable law, regulation, or order that form the basis for the determination.

(2) *Indirect air carrier reply.* The indirect air carrier may respond to the notice of proposed withdrawal of approval no later than 15 calendar days after receipt of the withdrawal by providing the designated official, in writing, with any material facts, arguments, applicable law, and regulation.

(3) *TSA review.* The designated official will consider all information available, including any relevant material or information submitted by the indirect air carrier, before either issuing a withdrawal of approval of the indirect air carrier's security program or rescinding the notice of proposed withdrawal of approval. If TSA issues a withdrawal of approval, it becomes effective upon receipt by the indirect air carrier, or 15 calendar days after service, whichever occurs first.

(4) *Petition for reconsideration.* The indirect air carrier may petition the TSA

to reconsider the withdrawal of approval by serving a petition for consideration no later than 15 calendar days after the indirect air carrier receives the withdrawal of approval. The indirect air carrier must serve the petition for reconsideration on the designated official. Submission of a petition for reconsideration will not automatically stay the withdrawal of approval. The indirect air carrier may request the designated official to stay the withdrawal of approval pending consideration of the petition.

(5) *Assistant Secretary's review.* The designated official transmits the petition together with all pertinent information to the Assistant Secretary for reconsideration. The Assistant Secretary will dispose of the petition within 15 calendar days of receipt by either directing the designated official to rescind the withdrawal of approval or by affirming the withdrawal of approval. The decision of the Assistant Secretary is a final order subject to judicial review in accordance with 49 U.S.C. 46110.

(6) *Emergency withdrawal.* If TSA finds that there is an emergency requiring immediate action, with respect to aviation security that makes procedures in this section contrary to the public interest, the designated official may issue an emergency withdrawal of the indirect air carrier's security program, without first issuing a notice of proposed withdrawal, effective without stay on the date that the indirect air carrier receives notice of the emergency withdrawal. In such a case, the designated official will send the indirect air carrier a brief statement of the facts, charges, and applicable law, regulation, or order that forms the basis for the emergency withdrawal. The indirect air carrier may submit a petition for reconsideration under the procedures in paragraphs (f)(2) through (f)(5) of this section; however, this petition will not stay the effective date of the emergency withdrawal.

(g) *Service of documents for withdrawal of approval of security program proceedings.* Service may be accomplished by personal delivery, certified mail, or express courier. Documents served on an indirect air carrier will be served at the indirect air carrier's official place of business as designated in its application for approval or its security program. Documents served on TSA must be served to the address noted in the notice of withdrawal of approval or withdrawal of approval, whichever is applicable.

(1) *Certificate of service.* An individual may attach a certificate of service to a document tendered for filing. A certificate of service must consist of a statement, dated and signed by the person filing the document, that the document was personally delivered, served by certified mail on a specific date, or served by express courier on a specific date.

(2) *Date of service.* The date of service will be—

(i) The date of personal delivery;

(ii) If served by certified mail, the mailing date shown on the certificate of service, the date shown on the postmark, if there is no certificate of service, or other mailing date shown by other evidence if there is no certificate of service or postmark; or

(iii) If served by express courier, the service date shown on the certificate of service, or by other evidence if there is no certificate of service.

(h) *Extension of time.* TSA may grant an extension of time of the limits set forth in this section for good cause shown. An indirect air carrier's request for an extension of time must be in writing and be received by TSA at least 2 days before the due date to be extended. TSA may grant itself an extension of time for good cause.

[71 FR 30513, May 26, 2006]

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1548.7 was amended by revising paragraph (f), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1548.7 Approval, amendment, annual renewal, and withdrawal of approval of the security program.

* * * * *

(f) *Withdrawal of approval of a security program.* Section 1540.301 includes procedures for withdrawal of approval of a security program.

* * * * *

§ 1548.9 Acceptance of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each indirect air carrier must use the facilities, equipment, and procedures described in its security program to prevent or deter the carriage onboard an aircraft of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item, as provided in the indirect air carrier's security program.

(b) *Refusal to transport.* Each indirect air carrier must refuse to offer for transport on an aircraft any cargo, if the shipper does not consent to a search or inspection of that cargo in accordance with this part, or parts 1544 or 1546 of this chapter.

[71 FR 30515, May 26, 2006]

§ 1548.11 Training and knowledge for individuals with security-related duties.

(a) No indirect air carrier may use an employee or agent to perform any security-related duties to meet the requirements of its security program, unless that individual has received training, as specified in its security program, including his or her personal responsibilities in § 1540.105 of this chapter.

(b) Each indirect air carrier must ensure that each of its authorized employees or agents who accept, handle, transport, or deliver cargo have knowledge of the—

(1) Applicable provisions of this part;

(2) Applicable Security Directives and Information Circulars;

(3) The approved airport security program(s) applicable to their location(s); and

(4) The aircraft operator's or indirect air carrier's security program, to the extent necessary in order to perform their duties.

(c) Each indirect air carrier must ensure that each of its authorized employees or agents under paragraph (b) of this section successfully completes recurrent training at least annually on their individual responsibilities in—

(1) Section 1540.105 of this chapter;

(2) The applicable provisions of this part;

(3) Applicable Security Directives and Information Circulars;

(4) The approved airport security program(s) applicable to their location(s); and

(5) The aircraft operator's or indirect air carrier's security program, to the extent that such individuals need to know in order to perform their duties.

(d) Operators must comply with the requirements of this section not later than November 22, 2006, for direct employees and not later than June 15, 2007, for agents.

[71 FR 30515, May 26, 2006, as amended at 71 FR 62549, Oct. 25, 2006]

§ 1548.13 Security coordinators.

Each indirect air carrier must designate and use an Indirect Air Carrier Security Coordinator (IACSC). The IACSC and alternates must be appointed at the corporate level and must serve as the indirect air carrier's primary contact for security-related activities and communications with TSA, as set forth in the security program. Either the IACSC or an alternate IACSC must be available on a 24-hour basis.

[71 FR 30515, May 26, 2006]

§ 1548.15 Access to Cargo: Security threat assessments for individuals having unescorted access to cargo.

This section applies to each indirect air carrier operating under this part.

(a) This section applies to each employee or agent the indirect air carrier authorizes to have unescorted access to cargo from the time—

(1) Cargo to be transported on an aircraft operated by an aircraft operator with a full all-cargo program under § 1544.101(h) of this chapter, or by a foreign air carrier under § 1546.101(e) of this chapter, reaches an indirect air carrier facility where the indirect air carrier consolidates or holds the cargo until the indirect air carrier transfers the cargo to an aircraft operator or foreign air carrier, or

(2) Cargo to be transported on an aircraft operated by an aircraft operator with a full program or by a foreign air carrier under § 1546.101(a) or (b) of this chapter, is accepted by the indirect air carrier.

(b) Before an indirect air carrier authorizes, and before an employee or

agent gains, unescorted access to cargo as described in paragraph (a) of this section, each employee or agent must successfully complete one of the following:

(1) A criminal history records check under §§1542.209, 1544.229, or 1544.230 of this chapter, if the individual is otherwise required to undergo that check.

(2) A Security Threat Assessment under part 1540 subpart C of this chapter. An employee or agent who has successfully completed this Security Threat Assessment for one employer need not complete it for another employer if the employee or agent has been continuously employed in a position that requires a Security Threat Assessment.

(3) Another Security Threat Assessment approved by TSA as comparable to paragraphs (b)(1) or (b)(2) of this section.

(c) Each indirect air carrier must ensure that each individual who has access to its cargo—

(1) Has successfully completed one of the checks in paragraph (b) of this section;

(2) Is escorted by a person who has successfully completed one of the checks in paragraph (b) of this section; or

(3) Is authorized to serve as law enforcement personnel at that location.

(d) Operators must submit to TSA the names and other identifying information required by TSA of all individuals required to successfully complete an assessment under paragraph (b) not later than May 15, 2007, for direct employees and not later than July 15, 2007, for agents. After those dates, the operators may not allow an individual to perform a function for which a STA is required, unless the operator has submitted the information for that individual to TSA.

(e) Operators must comply with the requirements of paragraphs (a), (b), and (c) of this section not later than the dates to be specified by TSA in a future rule in the FEDERAL REGISTER.

[71 FR 30516, May 26, 2006; 71 FR 31965, June 2, 2006, as amended at 71 FR 62549, Oct. 25, 2006; 72 FR 13026, Mar. 20, 2007]

EFFECTIVE DATE NOTE: At 74 FR 47705, Sept. 16, 2009, §1548.15 was revised, effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§1548.15 Access to cargo: Security threat assessments for individuals having unescorted access to cargo.

(a) Before an aircraft operator authorizes and before an individual performs a function described in paragraph (b) of this section—

(1) Each individual must successfully complete a security threat assessment or comparable security threat assessment described in part 1540 subpart C of this chapter; and

(2) Each aircraft operator must complete the requirements in part 1540 subpart C.

(b) The security threat assessment required in paragraph (a) of this section applies to the following:

(1) Each individual who has unescorted access to cargo and access to information that such cargo will be transported on a passenger aircraft; or who has unescorted access to cargo screened for transport on a passenger aircraft; or who performs certain functions related to the transportation, dispatch or security of cargo for transport on a passenger aircraft or all-cargo aircraft, as specified in the indirect air carrier's security program; from the time—

(i) Cargo to be transported on an all-cargo aircraft operated by an aircraft operator with a full all-cargo program under §1544.101(h) of this chapter, or by a foreign air carrier under §1546.101(e) of this chapter, reaches an indirect air carrier facility where the indirect air carrier consolidates or holds the cargo, until the indirect air carrier transfers the cargo to an aircraft operator or foreign air carrier; or

(ii) Cargo to be transported on a passenger aircraft operated by an aircraft operator with a full program under §1544.101(a) or by a foreign air carrier under §1546.101(a) or (b) of this chapter, is accepted by the indirect air carrier, until the indirect air carrier transfers the cargo to an aircraft operator or foreign air carrier.

(2) Each individual the indirect air carrier authorizes to screen cargo or to supervise the screening of cargo under §1548.21.

§1548.16 Security threat assessments for each proprietor, general partner, officer, director, and certain owners of the entity.

(a) Each indirect air carrier, or applicant to be an indirect air carrier, must ensure that the names and other identifying information required by TSA of each proprietor, general partner, officer, director, and owner of the entity have been submitted to TSA for a Security Threat Assessment under part 1540, subpart C, of this chapter not later than May 15, 2007. After those

dates, the operators may not allow an individual to perform this function unless the operator has submitted the information for that individual to TSA.

(b) For purposes of this section, *owner* means—

(1) A person who directly or indirectly owns, controls, or has power to vote 25 percent or more of any class of voting securities or other voting interests of an IAC or applicant to be an IAC; or

(2) 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 IAC, or applicant to be an IAC.

(c) For purposes of this definition of *owner*—

(1) Members of the same family must be considered to be one person.

(i) *Same family* means parents, spouses, children, siblings, uncles, aunts, grandparents, grandchildren, first cousins, stepchildren, stepsiblings, and parents-in-law, and spouses of any of the foregoing.

(ii) Each member of the same family, who has an ownership interest in an IAC, or an applicant to be an IAC, must be identified if the family is an owner as a result of aggregating the ownership interests of the members of the family.

(iii) In determining the ownership of interests of the same family, any voting interest of any family member must be taken into account.

(2) *Voting securities or other voting interests* means securities or other interests that entitle the holder to vote for or select directors (or individuals exercising similar functions).

(d) Each indirect air carrier, or applicant to be an indirect air carrier, must ensure that each proprietor, general partner, officer, director and owner of the entity has successfully completed a Security Threat Assessment under part 1540, subpart C, of this chapter not later than a date to be specified by TSA in a future rule in the FEDERAL REGISTER.

[71 FR 30516, May 26, 2006; 71 FR 31965, June 2, 2006, as amended at 71 FR 62550, Oct. 25, 2006; 72 FR 13026, Mar. 20, 2007]

EFFECTIVE DATE NOTE: At 74 FR 47706, Sept. 16, 2009, §1548.16 was amended by revising paragraph (a), effective November 16, 2009. For the convenience of the user, the revised text is set forth as follows:

§ 1548.16 Security threat assessments for each proprietor, general partner, officer, director, and certain owners of the entity.

(a) Before an indirect air carrier permits a proprietor, general partner, officer, director, or owner of the entity to perform those functions—

(1) The proprietor, general partner, officer, director, or owner of the entity must successfully complete a security threat assessment or comparable security threat assessment described in part 1540 subpart C of this chapter; and

(2) Each indirect air carrier must complete the requirements in 49 CFR part 1540, subpart C.

* * * * *

§ 1548.17 Known shipper program.

This section applies to cargo that an indirect air carrier offers to an aircraft operator operating under a full program under §1544.101(a) of this chapter, or to a foreign air carrier operating under §1546.101(a) or (b) of this chapter.

(a) For cargo to be loaded on aircraft in the United States, each indirect air carrier must have and carry out a known shipper program in accordance with its security program. The program must—

(1) Determine the shipper's validity and integrity as provided in its security program;

(2) Provide that the indirect air carrier will separate known shipper cargo from unknown shipper cargo.

(b) When required by TSA, each indirect air carrier must submit to TSA, in a form and manner acceptable to TSA—

(1) Information identified in its security program regarding an applicant to be a known shipper or a known shipper; and

(2) Corrections and updates of this information upon learning of a change to the information specified in paragraph (b)(1) of this section.

[71 FR 30516, May 26, 2006]

§ 1548.19 Security Directives and Information Circulars.

(a) TSA may issue an Information Circular to notify indirect air carriers of security concerns.

(b) When TSA determines that additional security measures are necessary to respond to a threat assessment, or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(1) Each indirect air carrier that is required to have an approved indirect air carrier security program must comply with each Security Directive that TSA issues to it, within the time prescribed in the Security Directive for compliance.

(2) Each indirect air carrier that receives a Security Directive must comply with the following:

(i) Within the time prescribed in the Security Directive, acknowledge in writing receipt of the Security Directive to TSA.

(ii) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(3) In the event that the indirect air carrier is unable to implement the measures in the Security Directive, the indirect air carrier must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval.

(i) The indirect air carrier must submit the proposed alternative measures within the time prescribed in the Security Directive.

(ii) The indirect air carrier must implement any alternative measures approved by TSA.

(4) Each indirect air carrier that receives a Security Directive may comment on it by submitting data, views, or arguments in writing to TSA.

(i) TSA may amend the Security Directive based on comments received.

(ii) Submission of a comment does not delay the effective date of the Security Directive.

(5) Each indirect air carrier that receives a Security Directive or Information Circular, and each person who receives information from a Security Directive or Information Circular, must:

(i) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with a need-to-know.

(ii) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those with a need-to-know without the prior written consent of TSA.

[71 FR 30516, May 26, 2006]

§ 1548.21 Screening of cargo.

An IAC may only screen cargo for transport on a passenger aircraft under §§ 1544.205 and 1546.205 if the IAC is a certified cargo screening facility as provided in part 1549.

[74 FR 47706, Sept. 16, 2009]

EFFECTIVE DATE NOTE: At 74 FR 47706, Sept. 16, 2009, § 1548.21 was added, effective November 16, 2009.

PART 1549—CERTIFIED CARGO SCREENING PROGRAM (Eff. 11-16-09)

Subpart A—General

Sec.

Subpart B—Operations

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44913–44914, 44916–44917, 44932, 44935–44936, 46105.

SOURCE: 74 FR 47706, Sept. 16, 2009, unless otherwise noted.

EFFECTIVE DATE NOTE: At 74 FR 47706, Sept. 16, 2009, part 1549 was added, effective Nov. 16, 2009.

Subpart A—General

§ 1549.1 Applicability.

This part applies to each facility applying for or certified by TSA as a certified cargo screening facility to screen cargo that will be transported on a passenger aircraft operated under a full program under 49 CFR 1544.101(a), or a foreign air carrier operating under a program under 49 CFR 1546.101(a) or (b).

§ 1549.3 TSA inspection authority.

(a) Each certified cargo screening facility must allow TSA, at any time or place, in a reasonable manner, without advance notice, to enter the facility and make any inspections or tests, including copying records, to—

(1) Determine compliance of a certified cargo screening facility, airport operator, foreign air carrier, indirect air carrier, or airport tenant with this chapter and 49 U.S.C. 114 and Subtitle VII, as amended; or

(2) Carry out TSA's statutory or regulatory authorities, including its authority to—

(i) Assess threats to transportation;

(ii) Enforce security-related regulations, directives, and requirements:

(iii) Inspect, maintain, and test the security of facilities, equipment, and systems;

(iv) Ensure the adequacy of security measures for the transportation of passengers and cargo;

(v) Oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

(vi) Review security plans; and

(vii) Carry out such other duties, and exercise such other powers, relating to transportation security as the Assistant Secretary of Homeland Security for the TSA considers appropriate, to the extent authorized by law.

(b) At the request of TSA, each certified cargo screening facility must provide evidence of compliance with this chapter, including copying records.

(c) TSA and DHS officials working with TSA may conduct inspections under this section without access media or identification media issued or approved by a certified cargo screening facility or other person, except that the TSA and DHS officials will have identification media issued by TSA or DHS.

§ 1549.5 Adoption and implementation of the security program.

(a) *Security program required.* No person may screen cargo to be tendered to an aircraft operator operating under a full program under part 1544, a foreign air carrier operating under §1546.101(a) or (b), or an indirect air carrier operating under §1548.5 for carriage on a passenger aircraft, unless that person holds and carries out an approved security program under this part.

(b) *Content.* Each security program under this part must—

(1) Provide for the security of the aircraft, as well as that of persons and property traveling in air transportation against acts of criminal violence and air piracy and against the introduction into the aircraft of any unauthorized explosive, incendiary, and other destructive substance or item as provided in the certified cargo screening facility's security program;

(2) Be designed to prevent or deter the introduction of any unauthorized explosive, incendiary, and other destructive substance or item onto an aircraft; and

(3) Include the procedures and description of the facilities and equipment used to comply with the requirements of this part.

(c) *Employees and agents.* The certified cargo screening facility must ensure that its employees and agents carry out the requirements of this chapter and the certified cargo screening facility's security program.

(d) *Facility's security program.* The certified cargo screening facility standard security program together with approved alternate procedures and amendments issued to a particular facility constitutes that facility's security program.

(e) *Availability.* Each certified cargo screening facility must:

(1) Maintain an original of the security program at its corporate office.

(2) Have accessible a complete copy, or the pertinent portions of its security program, or appropriate implementing instructions, at its facility. An electronic version is adequate.

(3) Make a copy of the security program available for inspection upon the request of TSA.

(4) Restrict the distribution, disclosure, and availability of information contained in its security program to persons with a need to know, as described in part 1520 of this chapter.

(5) Refer requests for such information by other persons to TSA.

§ 1549.7 Approval, amendment, renewal of the security program and certification of a certified cargo screening facility.

(a) *Initial application and approval*—(1) *Application.* Unless otherwise authorized by TSA, each applicant must apply for a security program and for certification as a certified cargo screening facility at a particular location, in a form and a manner prescribed by TSA not less than 90 calendar days before the applicant intends to begin operations. TSA will only approve a facility to operate as a CCSF if it is located in the United States. The CCSF application must be in writing and include the following:

(i) The business name; other names, including doing business as; state of incorporation, if applicable; and tax identification number.

(ii) The name of the senior manager or representative of the applicant in control of the operations at the facility.

(iii) A signed statement from each person listed in paragraph (a)(1)(ii) of this section stating whether he or she has been a senior manager or representative of a facility that had its security program withdrawn by TSA.

(iv) Copies of government-issued identification of persons listed in paragraph (a)(1)(ii) of this section.

(v) The street address of the facility where screening will be conducted.

(vi) A statement acknowledging and ensuring that each individual and agent of the applicant, who is subject to training under §1549.11, will have successfully completed the training outlined in its security program before performing security-related duties.

(vii) Other information requested by TSA concerning Security Threat Assessments.

(viii) A statement acknowledging and ensuring that each individual will successfully complete a Security Threat Assessment under §1549.111 before the applicant authorizes the individual to have unescorted access to screened cargo or to screen or supervise the screening of cargo.

(2) *Standard security program and assessment.* (i) After the Security Coordinator for an applicant successfully completes a security threat assessment, TSA will provide to the applicant the certified cargo screening standard security program, any security directives, and amendments to the security program and other alternative procedures that apply to the facility. The applicant may either accept the standard security program or submit a proposed modified security program to the designated official for approval. TSA will approve the security program under paragraphs (a)(3) and (a)(4) of the section or issue a written notice to modify under paragraph (a)(4) of this section.

(ii) An applicant must successfully undergo an assessment by a TSA-approved validation firm under 49 CFR part 1522 or by TSA.

(3) *Review.* TSA will review a facility at a particular location to determine whether—

(i) The applicant has met the requirements of this part, its security program, and any applicable Security Directive;

(ii) The applicant has successfully undergone an assessment by a TSA-approved validation firm under 49 CFR part 1522 or by TSA;

(iii) The applicant is able and willing to carry out the requirements of this part, its security program, and an applicable Security Directive;

(iv) The approval of such applicant's security program is not contrary to the interests of security and the public interest;

(v) The applicant has not held a security program that was withdrawn within the previous year, unless otherwise authorized by TSA; and

(vi) TSA determines that the applicant is qualified to be a certified cargo screening facility.

(4) *Approval and certification.* If TSA determines that the requirements of paragraph (a)(4) of this section are met and the application is approved, TSA

will send the applicant a written notice of approval of its security program, and certification to operate as a certified cargo screening facility.

(5) *Commencement of operations.* The certified cargo screening facility may operate under a security program when it meets all TSA requirements, including but not limited to a validation by TSA or a TSA-approved validation firm, successful completion of training, and Security Threat Assessments by relevant personnel.

(6) *Duration of security program.* The security program will remain effective until the end of the calendar month three years after the month it was approved or until the program has been surrendered or withdrawn, whichever is earlier.

(7) *Requirement to report changes in information.* Each certified cargo screening facility under this part must notify TSA, in a form and manner approved by TSA, of any changes to the information submitted during its initial application.

(i) The CCSF must submit this notification to TSA not later than 30 days prior to the date the change is expected to occur.

(ii) Changes included in the requirement of this paragraph include, but are not limited to, changes in the certified cargo screening facility's contact information, senior manager or representative, business addresses and locations, and form of business facility.

(iii) If the certified cargo screening facility relocates, TSA will withdraw the existing certification and require the new facility to undergo a validation and certification process.

(b) *Renewal Application.* Upon timely submittal of an application for renewal, and unless and until TSA denies the application, the certified cargo screening facility's approved security program remains in effect.

(1) Unless otherwise authorized by TSA, each certified cargo screening facility must timely submit to TSA, at least 30 calendar days prior to the first day of the 36th anniversary month of initial approval of its security program, an application for renewal of its security program in a form and a manner approved by TSA.

(2) The certified cargo screening facility must demonstrate that it has successfully undergone a revalidation of its operations by a TSA or a TSA-approved validation firm prior to the first day of the 36th anniversary month of initial approval of its security program.

(3) The application for renewal must be in writing and include a signed statement that the certified cargo screening facility has reviewed and ensures the continuing accuracy of the contents of its initial application for a security program, subsequent renewal applications, or other submissions to TSA confirming a change of information and noting the date such applications and submissions were sent to TSA, including the following certification:

> [Name of certified cargo screening facility] (hereinafter ''the CCSF'') has adopted and is currently carrying out a security program in accordance with the Transportation Security Regulations as originally approved on [Insert date of TSA initial approval]. In accordance with TSA regulations, the CCSF has notified TSA of any new or changed information required for the CCSF's initial security program. If new or changed information is being submitted to TSA as part of this application for reapproval, that information is stated in this filing.
>
> The CCSF understands that intentional falsification of certification to an aircraft operator, foreign air carrier, indirect air carrier, or to TSA may be subject to both civil and criminal penalties under 49 CFR part 1540 and 18 U.S.C. 1001. Failure to notify TSA of any new or changed information required for initial approval of the CCSF's security program in a timely fashion and in a form acceptable to TSA may result in withdrawal by TSA of approval of the CCSF's security program.

(4) TSA will renew approval of the security program if TSA determines that—

(i) The CCSF has met the requirements of this chapter, its security program, and any Security Directive; and

(ii) The renewal of its security program is not contrary to the interests of security and the public interest.

(5) If TSA determines that the certified cargo screening facility meets the requirements of paragraph (b)(3) of this section, it will renew the certified cargo screening facility's security program and certification. The security

program and certification will remain effective until the end of the calendar month three years after the month it was renewed.

(c) *Amendment requested by a certified cargo screening entity or applicant.* A certified cargo screening facility or applicant may file a request for an amendment to its security program with the TSA designated official at least 45 calendar days before the date it proposes for the amendment to become effective, unless the designated official allows a shorter period. Any certified cargo screening facility may submit to TSA a group proposal for an amendment that is on behalf of it and other certified cargo screening facilities that co-sign the proposal.

(1) Within 30 calendar days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(2) TSA may approve an amendment to a certified cargo screening facility's security program, if the TSA designated official determines that safety and the public interest will allow it, and if the proposed amendment provides the level of security required under this part.

(3) Within 30 calendar days after receiving a denial of the proposed amendment, the certified cargo screening facility may petition TSA to reconsider the denial. The CCSF must file the Petition for Reconsideration with the designated official.

(4) Upon receipt of a Petition for Reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to TSA for reconsideration. TSA will dispose of the petition within 30 calendar days of receipt by either directing the designated official to approve the amendment or by affirming the denial.

(d) *Amendment by TSA.* TSA may amend a security program in the interest of safety and the public interest, as follows:

(1) TSA notifies the certified cargo screening facility, in writing, of the proposed amendment, fixing a period of not less than 30 calendar days within which the certified cargo screening facility may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the certified cargo screening facility of any amendment adopted or rescinds the notice of amendment. If the amendment is adopted, it becomes effective not less than 30 calendar days after the certified cargo screening facility receives the notice of amendment, unless the certified cargo screening facility disagrees with the proposed amendment and petitions the TSA to reconsider, no later than 15 calendar days before the effective date of the amendment. The certified cargo screening facility must send the petition for reconsideration to the designated official. A timely Petition for Reconsideration stays the effective date of the amendment.

(3) Upon receipt of a Petition for Reconsideration, the designated official either amends or withdraws the notice of amendment, or transmits the Petition, together with any pertinent information, to TSA for reconsideration. TSA disposes of the Petition within 30 calendar days of receipt, either by directing the designated official to withdraw or amend the notice of amendment, or by affirming the notice of amendment.

(e) *Emergency amendments.* (1) If TSA finds that there is an emergency requiring immediate action, with respect to aviation security that makes procedures in this section contrary to the public interest, the designated official may issue an emergency amendment, without the prior notice and comment procedures described in paragraph (d) of this section.

(2) The emergency amendment is effective without stay on the date the certified cargo screening facility receives notification. TSA will incorporate in the notification a brief statement of the reasons and findings for the emergency amendment to be adopted.

(3) The certified cargo screening facility may file a Petition for Reconsideration with the TSA no later than 15 calendar days after TSA issued the emergency amendment. The certified cargo screening facility must send the Petition for Reconsideration to the

designated official; however, the filing does not stay the effective date of the emergency amendment.

Subpart B—Operations

§ 1549.101 Acceptance, screening, and transfer of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each certified cargo screening facility must use the facilities, equipment, and procedures described in its security program to prevent or deter the carriage onboard an aircraft of any unauthorized explosives, incendiaries, and other destructive substances or items in cargo onboard an aircraft, as provided in the facility's security program.

(b) *Screening and inspection of cargo.* Each certified cargo screening facility must ensure that cargo is screened and inspected for any unauthorized explosive, incendiary, and other destructive substance or item as provided in the facility's security program before it is tendered to another certified cargo screening facility, an aircraft operator with a full program under part 1544, a foreign air carrier operating under §§ 1546.101(a) or (b), or an indirect air carrier operating under § 1548.5 for transport on a passenger aircraft. Cargo that the facility represents as screened, must be screened in accordance with this part.

(c) *Refusal to transport.* Each certified cargo screening facility must refuse to offer to another certified cargo screening facility, an aircraft operator with a full program under part 1544, a foreign air carrier operating under §§ 1546.101(a) or (b), or an indirect air carrier operating under § 1548.5 for transport on a passenger aircraft any cargo, if the shipper does not consent to a search or inspection of that cargo in accordance with this part, or parts 1544, 1546, or 1548 of this chapter.

(d) *Chain of custody.* Each certified cargo screening facility must protect the cargo from unauthorized access from the time it is screened until the time it is tendered to another certified cargo screening facility as approved by TSA, an indirect air carrier under 49 CFR part 1548, an aircraft operator under part 1544, or a foreign air carrier under part 1546.

§ 1549.103 Qualifications and training of individuals with security-related duties.

(a) *Security threat assessments.* Each certified cargo screening facility must ensure that individuals listed in 49 CFR 1540.201(a)(6), (7), (8), (9), and (12) relating to a certified cargo screening facility complete a security threat assessment or comparable security threat assessment described in part 1540, subpart C of this chapter, before conducting screening or supervising screening or before having unescorted access to screened cargo, unless the individual is authorized to serve as law enforcement personnel at that location.

(b) *Training required.* Each certified cargo screening facility must ensure that individuals have received training, as specified in this section and its security program, before such individual perform any duties to meet the requirements of its security program.

(c) *Knowledge and training requirements.* Each certified cargo screening facility must ensure that each individual who performs duties to meet the requirements of its security program have knowledge of, and annual training in, the—

(1) Applicable provisions of this chapter, including this part, part 1520, and § 1540.105;

(2) The certified cargo screening facility's security program, to the extent that such individuals need to know in order to perform their duties;

(3) Applicable Security Directives and Information Circulars; and

(4) The applicable portions of approved airport security program(s) and aircraft operator security program(s).

(d) *Screener qualifications.* Each certified cargo screening facility must ensure that each individual who screens cargo or who supervises cargo screening—

(1) Is a citizen or national of the United States, or an alien lawfully admitted for permanent residence;

(2) Has a high school diploma, a General Equivalency Diploma, or a combination of education and experience that the certified cargo screening facility has determined to have equipped the person to perform the duties of the position;

(3) Has basic aptitudes and physical abilities including color perception, visual and aural acuity, physical coordination, and motor skills to the extent required to effectively operate cargo screening technologies that the facility is authorized to use. These include:

(i) The ability to operate x-ray equipment and to distinguish on the x-ray monitor the appropriate imaging standard specified in the certified cargo screening facility security program. Wherever the x-ray system displays colors, the operator must be able to perceive each color.

(ii) The ability to distinguish each color displayed on every type of screening equipment and explain what each color signifies.

(iii) The ability to hear and respond to the spoken voice and to audible alarms generated by screening equipment.

(4) Has the ability to read, write and understand English well enough to carry out written and oral instructions regarding the proper performance of screening duties or be under the direct supervision of someone who has this ability, including reading labels and shipping papers, and writing log entries into security records in English.

§ 1549.105 Recordkeeping.

(a) Each certified cargo screening facility must maintain records demonstrating compliance with all statutes, regulations, directives, orders, and security programs that apply to operation as a certified cargo screening facility, including the records listed below, at the facility location or other location as approved by TSA:

(1) Records of all training and instructions given to each individual under §1549.103. The CCSF must retain these records for 180 days after the individual is no longer employed by the certified cargo screening facility or is no longer acting as the facility's agent.

(2) Copies of all applications for, or renewals of, TSA certification to operate under part 1549. Copies of reports by TSA-certified validators must be included in these records.

(3) Documents establishing TSA's certification and renewal of certification as required by part 1549.

(4) Records demonstrating that each individual has complied with the security threat assessment provisions of §1549.111.

(b) Unless otherwise stated, records must be retained until the next re-certification.

§ 1549.107 Security coordinators.

Each certified cargo screening facility must have a Security Coordinator and designated alternate Security Coordinator appointed at the corporate level. In addition, each certified cargo screening facility must have a facility Security Coordinator and alternate facility Security Coordinator appointed at the facility level. The facility Security Coordinator must serve as the certified cargo screening facility's primary contact for security-related activities and communications with TSA, as set forth in the security program. The Security Coordinator and alternate appointed at the corporate level, as well as the facility Security Coordinator and alternate, must be available on a 24-hour, 7-days a week basis.

§ 1549.109 Security Directives and Information Circulars.

(a) TSA may issue an Information Circular to notify certified cargo screening facilities of security concerns.

(b) When TSA determines that additional security measures are necessary to respond to a threat assessment, or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(1) Each certified cargo screening facility must comply with each Security Directive that TSA issues to it, within the time prescribed in the Security Directive for compliance.

(2) Each certified cargo screening facility that receives a Security Directive must comply with the following:

(i) Within the time prescribed in the Security Directive, acknowledge in writing receipt of the Security Directive to TSA.

(ii) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(3) In the event that the certified cargo screening facility is unable to implement the measures in the Security Directive, the certified cargo screening facility must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval.

(i) The certified cargo screening facility must submit the proposed alternative measures within the time prescribed in the Security Directive.

(ii) The certified cargo screening facility must implement any alternative measures approved by TSA.

(4) Each certified cargo screening facility that receives a Security Directive may comment on it by submitting data, views, or arguments in writing to TSA.

(i) TSA may amend the Security Directive based on comments received.

(ii) Submission of a comment does not delay the effective date of the Security Directive.

(5) Each certified cargo screening facility that receives a Security Directive or Information Circular, and each person who receives information from a Security Directive or Information Circular, must—

(i) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with a need-to-know; and

(ii) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those with a need-to-know without the prior written consent of TSA.

§ 1549.111 Security threat assessments for personnel of certified cargo screening facilities.

(a) *Scope.* This section applies to the following:

(1) Each individual the certified cargo screening facility authorizes to perform cargo screening or supervise cargo screening.

(2) Each individual the certified cargo screening facility authorizes to have unescorted access to cargo at any time from the time it is screened until the time it is tendered to another certified cargo screening facility, an indirect air carrier under 49 CFR part 1548 for transport on a passenger aircraft, an aircraft operator under part 1544, or a foreign air carrier under part 1546.

(3) The senior manager or representative of its facility in control of the operations.

(4) The security coordinators and their alternates.

(b) *Security threat assessment.* Before a certified cargo screening facility authorizes an individual to perform the functions described in paragraph (a) of this section, and before the individual performs those functions—

(1) Each individual must successfully complete a security threat assessment or comparable security threat assessment described in part 1540, subpart C of this chapter; and

(2) Each certified screening facility must complete the requirements in 49 CFR part 1540, subpart C.

PART 1550—AIRCRAFT SECURITY UNDER GENERAL OPERATING AND FLIGHT RULES

Sec.

AUTHORITY: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

SOURCE: 67 FR 8383, Feb. 22, 2002, unless otherwise noted.

§ 1550.1 Applicability of this part.

This part applies to the operation of aircraft for which there are no security requirements in other parts of this subchapter.

§ 1550.3 TSA inspection authority.

(a) Each aircraft operator subject to this part must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance with—

(1) This subchapter and any security program or security procedures under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each aircraft operator must provide evidence of

compliance with this part and its security program or security procedures, including copies of records.

§ 1550.5 Operations using a sterile area.

(a) *Applicability of this section.* This section applies to all aircraft operations in which passengers, crewmembers, or other individuals are enplaned from or deplaned into a sterile area, except for scheduled passenger operations, public charter passenger operations, and private charter passenger operations, that are in accordance with a security program issued under part 1544 or 1546 of this chapter.

(b) *Procedures.* Any person conducting an operation identified in paragraph (a) of this section must conduct a search of the aircraft before departure and must screen passengers, crewmembers, and other individuals and their accessible property (carry-on items) before boarding in accordance with security procedures approved by TSA.

(c) *Sensitive security information.* The security program procedures approved by TSA for operations specified in paragraph (a) of this section are sensitive security information. The operator must restrict the distribution, disclosure, and availability of information contained in the security procedures to persons with a need to know as described in part 1520 of this chapter.

(d) *Compliance date.* Persons conducting operations identified in paragraph (a) of this section must implement security procedures on October 6, 2001.

(e) *Waivers.* TSA may permit a person conducting an operation under this section to deviate from the provisions of this section if TSA finds that the operation can be conducted safely under the terms of the waiver.

§ 1550.7 Operations in aircraft of 12,500 pounds or more.

(a) *Applicability of this section.* This section applies to each aircraft operation conducted in an aircraft with a maximum certificated takeoff weight of 12,500 pounds or more except for those operations specified in §1550.5 and those operations conducted under a security program under part 1544 or 1546 of this chapter.

(b) *Procedures.* Any person conducting an operation identified in paragraph (a) of this section must conduct a search of the aircraft before departure and screen passengers, crewmembers, and other persons and their accessible property (carry-on items) before boarding in accordance with security procedures approved by TSA.

(c) *Compliance date.* Persons identified in paragraph (a) of this section must implement security procedures when notified by TSA. TSA will notify operators by NOTAM, letter, or other communication when they must implement security procedures.

(d) *Waivers.* TSA may permit a person conducting an operation identified in this section to deviate from the provisions of this section if TSA finds that the operation can be conducted safely under the terms of the waiver.

PART 1552—FLIGHT SCHOOLS

Subpart A—Flight Training for Aliens and Other Designated Individuals

Subpart B—Flight School Security Awareness Training

AUTHORITY: 49 U.S.C. 114, 44939.

SOURCE: 69 FR 56340, Sept. 20, 2004, unless otherwise noted.

Subpart A—Flight Training for Aliens and Other Designated Individuals

§ 1552.1 Scope and definitions.

(a) *Scope.* This subpart applies to flight schools that provide instruction under 49 U.S.C. Subtitle VII, Part A, in the operation of aircraft or aircraft simulators, and individuals who apply to obtain such instruction or who receive such instruction.

(b) *Definitions.* As used in this part:

Aircraft simulator means a flight simulator or flight training device, as those terms are defined at 14 CFR 61.1.

Alien means any person not a citizen or national of the United States.

Candidate means an alien or other individual designated by TSA who applies for flight training or recurrent training. It does not include an individual endorsed by the Department of Defense for flight training.

Day means a day from Monday through Friday, including State and local holidays but not Federal holidays, for any time period less than 11 days specified in this part. For any time period greater than 11 days, day means calendar day.

Demonstration flight for marketing purposes means a flight for the purpose of demonstrating an aircraft's or aircraft simulator's capabilities or characteristics to a potential purchaser, or to an agent of a potential purchaser, of the aircraft or simulator, including an acceptance flight after an aircraft manufacturer delivers an aircraft to a purchaser.

Flight school means any pilot school, flight training center, air carrier flight training facility, or flight instructor certificated under 14 CFR part 61, 121, 135, 141, or 142; or any other person or entity that provides instruction under 49 U.S.C. Subtitle VII, Part A, in the operation of any aircraft or aircraft simulator.

Flight training means instruction received from a flight school in an aircraft or aircraft simulator. Flight training does not include recurrent training, ground training, a demonstration flight for marketing purposes, or any military training provided by the Department of Defense, the U.S. Coast Guard, or an entity under contract with the Department of Defense or U.S. Coast Guard.

Ground training means classroom or computer-based instruction in the operation of aircraft, aircraft systems, or cockpit procedures. Ground training does not include instruction in an aircraft simulator.

National of the United States means a person who, though not a citizen of the United States, owes permanent allegiance to the United States, and includes a citizen of American Samoa or Swains Island.

Recurrent training means periodic training required under 14 CFR part 61, 121,125, 135, or Subpart K of part 91. Recurrent training does not include training that would enable a candidate who has a certificate or type rating for a particular aircraft to receive a certificate or type rating for another aircraft.

§ 1552.3 Flight training.

This section describes the procedures a flight school must follow before providing flight training.

(a) *Category 1—Regular processing for flight training on aircraft more than 12,500 pounds.* A flight school may not provide flight training in the operation of any aircraft having a maximum certificated takeoff weight of more than 12,500 pounds to a candidate, except for a candidate who receives expedited processing under paragraph (b) of this section, unless—

(1) The flight school has first notified TSA that the candidate has requested such flight training.

(2) The candidate has submitted to TSA, in a form and manner acceptable to TSA, the following:

(i) The candidate's full name, including any aliases used by the candidate or variations in the spelling of the candidate's name;

(ii) A unique candidate identification number created by TSA;

(iii) A copy of the candidate's current, unexpired passport and visa;

(iv) The candidate's passport and visa information, including all current and previous passports and visas held by the candidate and all the information necessary to obtain a passport and visa;

(v) The candidate's country of birth, current country or countries of citizenship, and each previous country of citizenship, if any;

(vi) The candidate's actual date of birth or, if the candidate does not know his or her date of birth, the approximate date of birth used consistently by the candidate for his or her passport or visa;

(vii) The candidate's requested dates of training and the location of the training;

(viii) The type of training for which the candidate is applying, including the aircraft type rating the candidate would be eligible to obtain upon completion of the training;

(ix) The candidate's current U.S. pilot certificate, certificate number, and type rating, if any;

(x) Except as provided in paragraph (k) of this section, the candidate's fingerprints, in accordance with paragraph (f) of this section;

(xi) The candidate's current address and phone number and each address for the 5 years prior to the date of the candidate's application;

(xii) The candidate's gender; and

(xiii) Any fee required under this part.

(3) The flight school has submitted to TSA, in a form and manner acceptable to TSA, a photograph of the candidate taken when the candidate arrives at the flight school for flight training.

(4) TSA has informed the flight school that the candidate does not pose a threat to aviation or national security, or more than 30 days have elapsed since TSA received all of the information specified in paragraph (a)(2) of this section.

(5) The flight school begins the candidate's flight training within 180 days of either event specified in paragraph (a)(4) of this section.

(b) *Category 2—Expedited processing for flight training on aircraft more than 12,500 pounds.* (1) A flight school may not provide flight training in the operation of any aircraft having a maximum certificated takeoff weight of more than 12,500 pounds to a candidate who meets any of the criteria of paragraph (b)(2) of this section unless—

(i) The flight school has first notified TSA that the candidate has requested such flight training.

(ii) The candidate has submitted to TSA, in a form and manner acceptable to TSA:

(A) The information and fee required under paragraph (a)(2) of this section; and

(B) The reason the candidate is eligible for expedited processing under paragraph (b)(2) of this section and information that establishes that the candidate is eligible for expedited processing.

(iii) The flight school has submitted to TSA, in a form and manner acceptable to TSA, a photograph of the candidate taken when the candidate arrives at the flight school for flight training.

(iv) TSA has informed the flight school that the candidate does not pose a threat to aviation or national security or more than 5 days have elapsed since TSA received all of the information specified in paragraph (a)(2) of this section.

(v) The flight school begins the candidate's flight training within 180 days of either event specified in paragraph (b)(1)(iv) of this section.

(2) A candidate is eligible for expedited processing if he or she—

(i) Holds an airman's certificate from a foreign country that is recognized by the Federal Aviation Administration or a military agency of the United States, and that permits the candidate to operate a multi-engine aircraft that has a certificated takeoff weight of more than 12,500 pounds;

(ii) Is employed by a foreign air carrier that operates under 14 CFR part 129 and has a security program approved under 49 CFR part 1546;

(iii) Has unescorted access authority to a secured area of an airport under 49 U.S.C. 44936(a)(1)(A)(ii), 49 CFR 1542.209, or 49 CFR 1544.229;

(iv) Is a flightcrew member who has successfully completed a criminal history records check in accordance with 49 CFR 1544.230; or

(v) Is part of a class of individuals that TSA has determined poses a minimal threat to aviation or national security because of the flight training already possessed by that class of individuals.

(c) *Category 3—Flight training on aircraft 12,500 pounds or less.* A flight school may not provide flight training in the operation of any aircraft having a maximum certificated takeoff weight of 12,500 pounds or less to a candidate unless—

(1) The flight school has first notified TSA that the candidate has requested such flight training.

(2) The candidate has submitted to TSA, in a form and manner acceptable to TSA:

(i) The information required under paragraph (a)(2) of this section; and

(ii) Any other information required by TSA.

(3) The flight school has submitted to TSA, in a form and manner acceptable to TSA, a photograph of the candidate taken when the candidate arrives at the flight school for flight training.

(4) The flight school begins the candidate's flight training within 180 days of the date the candidate submitted the information required under paragraph (a)(2) of this section to TSA.

(d) *Category 4—Recurrent training for all aircraft.* Prior to beginning recurrent training for a candidate, a flight school must—

(1) Notify TSA that the candidate has requested such recurrent training; and

(2) Submit to TSA, in a form and manner acceptable to TSA:

(i) The candidate's full name, including any aliases used by the candidate or variations in the spelling of the candidate's name;

(ii) Any unique student identification number issued to the candidate by the Department of Justice or TSA;

(iii) A copy of the candidate's current, unexpired passport and visa;

(iv) The candidate's current U.S. pilot certificate, certificate number, and type rating(s);

(v) The type of training for which the candidate is applying;

(vi) The date of the candidate's prior recurrent training, if any, and a copy of the training form documenting that recurrent training;

(vii) The candidate's requested dates of training; and

(viii) A photograph of the candidate taken when the candidate arrives at the flight school for flight training.

(e) *Interruption of flight training.* A flight school must immediately terminate or cancel a candidate's flight training if TSA notifies the flight school at any time that the candidate poses a threat to aviation or national security.

(f) *Fingerprints.* (1) Fingerprints submitted in accordance with this subpart must be collected—

(i) By United States Government personnel at a United States embassy or consulate; or

(ii) By another entity approved by TSA.

(2) A candidate must confirm his or her identity to the individual or agency collecting his or her fingerprints under paragraph (f)(1) of this section by providing the individual or agency his or her:

(i) Passport;

(ii) Resident alien card; or

(iii) U.S. driver's license.

(3) A candidate must pay any fee imposed by the agency taking his or her fingerprints.

(g) *General requirements*—(1) *False statements.* If a candidate makes a knowing and willful false statement, or omits a material fact, when submitting the information required under this part, the candidate may be—

(i) Subject to fine or imprisonment or both under 18 U.S.C. 1001;

(ii) Denied approval for flight training under this section; and

(iii) Subject to other enforcement action, as appropriate.

(2) *Preliminary approval.* For purposes of facilitating a candidate's visa process with the U.S. Department of State, TSA may inform a flight school and a candidate that the candidate has received preliminary approval for flight training based on information submitted by the flight school or the candidate under this section. A flight school may then issue an I–20 form to the candidate to present with the candidate's visa application. Preliminary approval does not initiate the waiting period under paragraph (a)(3) or (b)(1)(iii) of this section or the period in which a flight school must initiate a candidate's training after receiving TSA approval under paragraph (a)(4) or (b)(1)(iv) of this section.

(h) *U.S. citizens and nationals and Department of Defense endorsees.* A flight school must determine whether an individual is a citizen or national of the United States, or a Department of Defense endorsee, prior to providing flight training to the individual.

(1) *U.S. citizens and nationals.* To establish U.S. citizenship or nationality an individual must present to the flight school his or her:

(i) Valid, unexpired United States passport;

(ii) Original or government-issued certified birth certificate of the United States, American Samoa, or Swains Island, together with a government-issued picture identification of the individual;

(iii) Original United States naturalization certificate with raised seal, or a Certificate of Naturalization issued by the U.S. Citizenship and Immigration Services (USCIS) or the U.S. Immigration and Naturalization Service (INS) (Form N–550 or Form N–570), together with a government-issued picture identification of the individual;

(iv) Original certification of birth abroad with raised seal, U.S. Department of State Form FS–545, or U.S. Department of State Form DS–1350, together with a government-issued picture identification of the individual;

(v) Original certificate of United States citizenship with raised seal, a Certificate of United States Citizenship issued by the USCIS or INS (Form N–560 or Form N–561), or a Certificate of Repatriation issued by the USCIS or INS (Form N–581), together with a government-issued picture identification of the individual; or

(vi) In the case of flight training provided to a Federal employee (including military personnel) pursuant to a contract between a Federal agency and a flight school, the agency's written certification as to its employee's United States citizenship or nationality, together with the employee's government-issued credentials or other Federally-issued picture identification.

(2) *Department of Defense endorsees.* To establish that an individual has been endorsed by the U.S. Department of Defense for flight training, the individual must present to the flight school a written statement acceptable to TSA from the U.S. Department of Defense attaché in the individual's country of residence together with a government-issued picture identification of the individual.

(i) *Recordkeeping requirements.* A flight school must—

(1) Maintain the following information for a minimum of 5 years:

(i) For each candidate:

(A) A copy of the photograph required under paragraph (a)(3), (b)(1)(iii), (c)(3), or (d)(2)(viii) of this section; and

(B) A copy of the approval sent by TSA confirming the candidate's eligibility for flight training.

(ii) For a Category 1, Category 2, or Category 3 candidate, a copy of the information required under paragraph (a)(2) of this section, except the information in paragraph (a)(2)(x).

(iii) For a Category 4 candidate, a copy of the information required under paragraph (d)(2) of this section.

(iv) For an individual who is a United States citizen or national, a copy of the information required under paragraph (h)(1) of this section.

(v) For an individual who has been endorsed by the U.S. Department of Defense for flight training, a copy of the information required under paragraph (h)(2) of this section.

(vi) A record of all fees paid to TSA in accordance with this part.

(2) Permit TSA and the Federal Aviation Administration to inspect the records required by paragraph (i)(1) of this section during reasonable business hours.

(j) *Candidates subject to the Department of Justice rule.* A candidate who submits a completed Flight Training Candidate Checks Program form and fingerprints to the Department of Justice in accordance with 28 CFR part 105 before September 28, 2004, or a later date specified by TSA, is processed in accordance with the requirements of that part. If TSA specifies a date later than the compliance dates identified in this part, individuals and flight schools who comply with 28 CFR part 105 up to that date will be considered to be in compliance with the requirements of this part.

(k) *Additional or missed flight training.* (1) A Category 1, 2, or 3 candidate who has been approved for flight training by TSA may take additional flight training without submitting fingerprints as specified in paragraph (a)(2)(x) of this section if the candidate:

(i) Submits all other information required in paragraph (a)(2) of this section, including the fee; and

(ii) Waits for TSA approval or until the applicable waiting period expires before initiating the additional flight training.

(2) A Category 1, 2, or 3 candidate who is approved for flight training by TSA, but does not initiate that flight training within 180 days, may reapply for flight training without submitting fingerprints as specified in paragraph (a)(2)(x) of this section if the candidate submits all other information required in paragraph (a)(2) of this section, including the fee.

§ 1552.5 Fees.

(a) *Imposition of fees.* The following fee is required for TSA to conduct a security threat assessment for a candidate for flight training subject to the requirements of § 1552.3: $130.

(b) *Remittance of fees.* (1) A candidate must remit the fee required under this subpart to TSA, in a form and manner acceptable to TSA, each time the candidate or the flight school is required to submit the information required under § 1552.3 to TSA.

(2) TSA will not issue any fee refunds, unless a fee was paid in error.

Subpart B—Flight School Security Awareness Training

§ 1552.21 Scope and definitions.

(a) *Scope.* This subpart applies to flight schools that provide instruction under 49 U.S.C. Subtitle VII, Part A, in the operation of aircraft or aircraft simulators, and to employees of such flight schools.

(b) *Definitions:* As used in this subpart:

Flight school employee means a flight instructor or ground instructor certificated under 14 CFR part 61, 141, or 142; a chief instructor certificated under 14 CFR part 141; a director of training certificated under 14 CFR part 142; or any other person employed by a flight school, including an independent contractor, who has direct contact with a flight school student. This includes an independent or solo flight instructor certificated under 14 CFR part 61.

§ 1552.23 Security awareness training programs.

(a) *General.* A flight school must ensure that—

(1) Each of its flight school employees receives initial and recurrent security awareness training in accordance with this subpart; and

(2) If an instructor is conducting the initial security awareness training program, the instructor has first successfully completed the initial flight school security awareness training program offered by TSA or an alternative initial flight school security awareness training program that meets the criteria of paragraph (c) of this section.

(b) *Initial security awareness training program.* (1) A flight school must ensure that—

(i) Each flight school employee employed on January 18, 2005 receives initial security awareness training in accordance with this subpart by January 18, 2005; and

(ii) Each flight school employee hired after January 18, 2005 receives initial security awareness training within 60 days of being hired.

(2) In complying with paragraph (b)(2) of this section, a flight school may use either:

(i) The initial flight school security awareness training program offered by TSA; or

(ii) An alternative initial flight school security awareness training program that meets the criteria of paragraph (c) of this section.

(c) *Alternative initial security awareness training program.* At a minimum, an alternative initial security awareness training program must—

(1) Require active participation by the flight school employee receiving the training.

(2) Provide situational scenarios requiring the flight school employee receiving the training to assess specific situations and determine appropriate courses of action.

(3) Contain information that enables a flight school employee to identify—

(i) Uniforms and other identification, if any are required at the flight school, for flight school employees or other persons authorized to be on the flight school grounds.

(ii) Behavior by clients and customers that may be considered suspicious, including, but not limited to:

(A) Excessive or unusual interest in restricted airspace or restricted ground structures;

(B) Unusual questions or interest regarding aircraft capabilities;

(C) Aeronautical knowledge inconsistent with the client or customer's existing airman credentialing; and

(D) Sudden termination of the client or customer's instruction.

(iii) Behavior by other on-site persons that may be considered suspicious, including, but not limited to:

(A) Loitering on the flight school grounds for extended periods of time; and

(B) Entering ''authorized access only'' areas without permission.

(iv) Circumstances regarding aircraft that may be considered suspicious, including, but not limited to:

(A) Unusual modifications to aircraft, such as the strengthening of landing gear, changes to the tail number, or stripping of the aircraft of seating or equipment;

(B) Damage to propeller locks or other parts of an aircraft that is inconsistent with the pilot training or aircraft flight log; and

(C) Dangerous or hazardous cargo loaded into an aircraft.

(v) Appropriate responses for the employee to specific situations, including:

(A) Taking no action, if a situation does not warrant action;

(B) Questioning an individual, if his or her behavior may be considered suspicious;

(C) Informing a supervisor, if a situation or an individual's behavior warrants further investigation;

(D) Calling the TSA General Aviation Hotline; or

(E) Calling local law enforcement, if a situation or an individual's behavior could pose an immediate threat.

(vi) Any other information relevant to security measures or procedures at the flight school, including applicable information in the TSA Information Publication ''Security Guidelines for General Aviation Airports''.

(d) *Recurrent security awareness training program.* (1) A flight school must ensure that each flight school employee receives recurrent security awareness training each year in the same month as the month the flight school employee received initial security awareness training in accordance with this subpart.

(2) At a minimum, a recurrent security awareness training program must contain information regarding—

(i) Any new security measures or procedures implemented by the flight school;

(ii) Any security incidents at the flight school, and any lessons learned as a result of such incidents;

(iii) Any new threats posed by or incidents involving general aviation aircraft contained on the TSA Web site; and

(iv) Any new TSA guidelines or recommendations concerning the security of general aviation aircraft, airports, or flight schools.

§ 1552.25 Documentation, recordkeeping, and inspection.

(a) *Documentation.* A flight school must issue a document to each flight school employee each time the flight school employee receives initial or recurrent security awareness training in accordance with this subpart. The document must—

(1) Contain the flight school employee's name and a distinct identification number.

(2) Indicate the date on which the flight school employee received the security awareness training.

(3) Contain the name of the instructor who conducted the training, if any.

(4) Contain a statement certifying that the flight school employee received the security awareness training.

(5) Indicate the type of training received, initial or recurrent.

(6) Contain a statement certifying that the alternative training program used by the flight school meets the criteria in 49 CFR 1552.23(c), if the flight school uses an alternative training program to comply with this subpart.

(7) Be signed by the flight school employee and an authorized official of the flight school.

(b) *Recordkeeping requirements.* A flight school must establish and maintain the following records for one year after an individual no longer is a flight school employee:

(1) A copy of the document required by paragraph (a) of this section for the initial and each recurrent security awareness training conducted for each

flight school employee in accordance with this subpart; and

(2) The alternative flight school security awareness training program used by the flight school, if the flight school uses such a program.

(c) *Inspection*. A flight school must permit TSA and the Federal Aviation Administration to inspect the records required under paragraph (b) of this section during reasonable business hours.

PART 1560—SECURE FLIGHT PROGRAM

Subpart A—General

Sec.

Subpart B—Collection and Transmission of Secure Flight Passenger Data for Watch List Matching

Subpart C—Passenger Redress

AUTHORITY: 49 U.S.C. 114, 40113, 44901, 44902, 44903.

SOURCE: 73 FR 64061, Oct. 28, 2008, unless otherwise noted.

Subpart A—General

§ 1560.1 Scope, purpose, and implementation.

(a) *Scope*. This part applies to the following:

(1) Aircraft operators required to adopt a full program under 49 CFR 1544.101(a).

(2) Foreign air carriers required to adopt a security program under 49 CFR 1546.101(a) or (b).

(3) Airport operators that seek to authorize individuals to enter a sterile area for purposes approved by TSA.

(4) Individuals who seek redress in accordance with subpart C of this part.

(b) *Purpose*. The purpose of this part is to enhance the security of air travel within the United States and support the Federal government's counterterrorism efforts by assisting in the detection of individuals identified on Federal government watch lists who seek to travel by air, and to facilitate the secure travel of the public. This part enables TSA to operate a watch list matching program known as Secure Flight, which involves the comparison of passenger and non-traveler information with the identifying information of individuals on Federal government watch lists.

(c) *Implementation*. Each covered aircraft operator must begin requesting the information described in §1560.101(a)(1) and have the capability to transmit SFPD to TSA in accordance with its Aircraft Operator Implementation Plan (AOIP) as approved by TSA. Each covered aircraft operator must begin transmitting information to TSA as required in §1560.101(b) on the date specified in, and in accordance with, its AOIP as approved by TSA. TSA will inform each covered aircraft operator 60 days prior to the date on which TSA will assume the watch list matching function from that aircraft operator.

§ 1560.3 Terms used in this part.

In addition to the terms in §§1500.3 and 1540.5 of this chapter, the following terms apply to this part:

Aircraft Operator Implementation Plan or *AOIP* means a written procedure describing how and when a covered aircraft operator or airport operator transmits passenger and flight information and non-traveler information to TSA, as well as other related matters.

Airport code means the official code, designated by the International Air Transport Association (IATA), for an airport.

Consolidated User Guide means a document developed by the Department of Homeland Security (DHS) to provide guidance to aircraft operators that

must transmit passenger information to one or more components of DHS on operational processing and transmission of passenger information to all required components in a unified manner. The Consolidated User Guide is part of the covered aircraft operator's security program.

Covered aircraft operator means each aircraft operator required to carry out a full program under 49 CFR 1544.101(a) or a security program under 49 CFR 1546.101(a) or (b).

Covered airport operator means each airport operator that seeks to authorize non-traveling individuals to enter a sterile area for a purpose permitted by TSA.

Covered flight means any operation of an aircraft that is subject to or operates under a full program under 49 CFR 1544.101(a). *Covered flight* also means any operation of an aircraft that is subject to or operates under a security program under 49 CFR 1546.101(a) or (b) arriving in or departing from the United States, or overflying the continental United States. *Covered flight* does not include any flight for which TSA has determined that the Federal government is conducting passenger matching comparable to the matching conducted pursuant to this part.

Date of birth means the day, month, and year of an individual's birth.

Department of Homeland Security Traveler Redress Inquiry Program or *DHS TRIP* means the voluntary program through which individuals may request redress if they believe they have been:

(1) Denied or delayed boarding transportation due to DHS screening programs;

(2) Denied or delayed entry into or departure from the United States at a port of entry; or

(3) Identified for additional (secondary) screening at U.S. transportation facilities, including airports, and seaports.

Full name means an individual's full name as it appears on a verifying identity document held by the individual.

Inhibited status means the status of a passenger or non-traveling individual to whom TSA has instructed a covered aircraft operator or a covered airport operator not to issue a boarding pass or to provide access to the sterile area.

Itinerary information means information reflecting a passenger's or non-traveling individual's itinerary specified in the covered aircraft operator's AOIP. For non-traveling individuals, itinerary information is the airport code for the sterile area to which the non-traveler seeks access. For passengers, itinerary information includes the following:

(1) Departure airport code.

(2) Aircraft operator.

(3) Scheduled departure date.

(4) Scheduled departure time.

(5) Scheduled arrival date.

(6) Scheduled arrival time.

(7) Arrival airport code.

(8) Flight number.

(9) Operating carrier (if available).

Known Traveler Number means a unique number assigned to an individual for whom the Federal government has conducted a security threat assessment and determined does not pose a security threat.

Non-traveling individual or *non-traveler* means an individual to whom a covered aircraft operator or covered airport operator seeks to issue an authorization to enter the sterile area of an airport in order to escort a minor or a passenger with disabilities or for some other purpose permitted by TSA. The term *non-traveling individual* or *non-traveler* does not include employees or agents of airport or aircraft operators or other individuals whose access to a sterile area is governed by another TSA requirement.

Overflying the continental United States means departing from an airport or location outside the United States and transiting the airspace of the continental United States en route to another airport or location outside the United States. Airspace of the continental United States includes the airspace over the lower 48 states of the United States, not including Alaska or Hawaii, and the airspace overlying the territorial waters between the U.S. coast of the lower 48 states and 12 nautical miles from the continental U.S. coast. *Overflying the continental United States* does not apply to:

(1) Flights that transit the airspace of the continental United States between two airports or locations in the

same country, where that country is Canada or Mexico; or

(2) Any other category of flights that the Assistant Secretary of Homeland Security (Transportation Security Administration) designates in a notice in the FEDERAL REGISTER.

Passenger means an individual who is traveling on a covered flight. The term *passenger* does not include:

(1) A crew member who is listed as a crew member on the flight manifest; or

(2) An individual with flight deck privileges under 49 CFR 1544.237 traveling on the flight deck.

Passenger Resolution Information or *PRI* means the information that a covered aircraft operator or covered airport operator transmits to TSA for an individual who TSA places in an inhibited status and from whom the covered aircraft operator or covered airport operator is required to request additional information and a Verifying Identity Document. *Passenger Resolution Information* includes, but is not limited to, the following:

(1) Covered aircraft operator's agent identification number or agent sine.

(2) Type of Verifying Identity Document presented by the passenger.

(3) The identification number on the Verifying Identity Document.

(4) Issue date of the Verifying Identity Document.

(5) Name of the governmental authority that issued the Verifying Identity Document.

(6) Physical attributes of the passenger such as height, eye color, or scars, if requested by TSA.

Passport information means the following information from an individual's passport:

(1) Passport number.

(2) Country of issuance.

(3) Expiration date.

(4) Gender.

(5) Full name.

Redress Number means the number assigned by DHS to an individual processed through the redress procedures described in 49 CFR part 1560, subpart C.

Secure Flight Passenger Data or (*SFPD*) means information regarding a passenger or non-traveling individual that a covered aircraft operator or covered airport operator transmits to TSA, to the extent available, pursuant to §1560.101. *SFPD* is the following information regarding a passenger or non-traveling individual:

(1) Full name.

(2) Date of birth.

(3) Gender.

(4) Redress number or Known Traveler Number (once implemented).

(5) Passport information.

(6) Reservation control number.

(7) Record sequence number.

(8) Record type.

(9) Passenger update indicator.

(10) Traveler reference number.

(11) Itinerary information.

Self-service kiosk means a kiosk operated by a covered aircraft operator that is capable of accepting a passenger reservation or a request for authorization to enter a sterile area from a non-traveling individual.

Sterile area means ''sterile area'' as defined in 49 CFR 1540.5.

Terrorist Screening Center or *TSC* means the entity established by the Attorney General to carry out Homeland Security Presidential Directive 6 (HSPD–6), dated September 16, 2003, to consolidate the Federal government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes.

Verifying Identity Document means one of the following documents:

(1) An unexpired passport issued by a foreign government.

(2) An unexpired document issued by a U.S. Federal, State, or tribal government that includes the following information for the individual:

(i) Full name.

(ii) Date of birth.

(iii) Photograph.

(3) Such other documents that TSA may designate as valid verifying identity documents.

Watch list refers to the No Fly and Selectee List components of the Terrorist Screening Database maintained by the Terrorist Screening Center. For certain flights, the ''watch list'' may include the larger set of watch lists maintained by the Federal government as warranted by security considerations.

Subpart B—Collection and Transmission of Secure Flight Passenger Data for Watch List Matching

§ 1560.101 Request for and transmission of information to TSA.

(a) *Request for information.* (1) Each covered aircraft operator must request the full name, gender, date of birth, and Redress Number for passengers on a covered flight and non-traveling individuals seeking access to an airport sterile area. For reservations made 72 hours prior to the scheduled time of departure for each covered flight, the covered aircraft operator must collect full name, gender, and date of birth for each passenger when the reservation is made or at a time no later than 72 hours prior to the scheduled time of departure of the covered flight. For an individual that makes a reservation for a covered flight within 72 hours of the scheduled time of departure for the covered flight, the covered aircraft operator must collect the individual's full name, date of birth, and gender at the time of reservation. The covered aircraft operator must include the information provided by the individual in response to this request in the SFPD.

(i) Except as provided in paragraph (a)(1)(ii) of this section, each covered aircraft operator must begin requesting the information described in paragraph (a)(1) of this section in accordance with its AOIP as approved by TSA.

(ii) An aircraft operator that becomes a covered aircraft operator after the effective date of this part must begin requesting the information on the date it becomes a covered aircraft operator.

(2) Beginning on a date no later than 30 days after being notified in writing by TSA, each covered aircraft operator must additionally request the Known Traveler Number for passengers on a covered flight and non-traveling individuals seeking access to an airport sterile area. The covered aircraft operator must include the Known Traveler Number provided by the passenger in response to this request in the SFPD.

(3) Each covered aircraft operator may not submit SFPD for any passenger on a covered flight who does not provide a full name, date of birth and gender. Each covered aircraft operator may not accept a request for authorization to enter a sterile area from a non-traveling individual who does not provide a full name, date of birth and gender.

(4) Each covered aircraft operator must ensure that each third party that accepts a reservation, or accepts a request for authorization to enter a sterile area, on the covered aircraft operator's behalf complies with the requirements of this section.

(5) If the covered aircraft operator also has an operation of an aircraft that is subject to 49 CFR 1544.101(b) through (i), the covered aircraft operator may submit SFPD for passengers on these operations for watch list matching under this part, provided that the covered aircraft operator—

(i) Collects and transmits the SFPD for the passengers in accordance with this section;

(ii) Provides the privacy notice to the passengers in accordance with 49 CFR 1560.103; and

(iii) Complies with the requirements of 49 CFR 1560.105 and 1560.107.

(b) *Transmission of Secure Flight Passenger Data to TSA.* Beginning on the date provided in a covered aircraft operator's AOIP, the covered aircraft operator must electronically transmit SFPD to TSA, prior to the scheduled departure of each covered flight, in accordance with its AOIP as approved by TSA.

(1) To the extent available, each covered aircraft operator must electronically transmit SFPD to TSA for each passenger on a covered flight.

(2) Each covered aircraft operator must transmit SFPD to TSA prior to the scheduled flight departure time, in accordance with its AOIP as approved by TSA.

(c) *Transmission of non-traveler information to TSA.* Beginning on the date provided in a covered aircraft operator's AOIP, the covered aircraft operator must electronically transmit SFPD to TSA for each non-traveling individual, prior to authorizing access to an airport sterile area.

(d) *Retransmission of information.* Each covered aircraft operator must retransmit to TSA updates to the information listed in paragraphs (b) and (c) of this section to reflect most recent changes to that information, as specified in its AOIP as approved by TSA.

§ 1560.103 Privacy notice.

(a) *Electronic collection of information*—(1) *Current electronic collection of information.* Prior to collecting information through a Web site or self-service kiosk from a passenger or non-traveling individual in order to comply with § 1560.101(a), a covered aircraft operator must make available the complete privacy notice set forth in paragraph (b) of this section.

(2) *Other electronic collection of information.* If a covered aircraft operator collects information directly from a passenger or non-traveling individual in order to comply with § 1560.101(a) through an electronic means not described in paragraph (a)(1) of this section, the covered aircraft operator must make available the complete privacy notice set forth in paragraph (b) of this section.

(3) *Third party Web site.* Each covered aircraft operator must ensure that each third party that maintains a Web site capable of making a reservation for the covered aircraft operator's reservation system, make available on its Web site the complete privacy notice set forth in paragraph (b) of this section prior to collecting information through the Web site.

(b) *Privacy notice.* The covered aircraft operator may substitute its name for the word ''us,'' but the complete privacy notice otherwise must be identical to the following paragraph unless TSA has approved alternative language:

The Transportation Security Administration of the U.S. Department of Homeland Security requires us to collect information from you for purposes of watch list screening, under the authority of 49 U.S.C. section 114, and the Intelligence Reform and Terrorism Prevention Act of 2004. Providing this information is voluntary; however, if it is not provided, you may be subject to additional screening or denied transport or authorization to enter a sterile area. TSA may share information you provide with law enforcement or intelligence agencies or others under its published system of records notice. For more on TSA Privacy policies, or to view the system of records notice and the privacy impact assessment, please see TSA's Web site at *www.tsa.gov*.

§ 1560.105 Denial of transport or sterile area access; designation for enhanced screening.

(a) *Applicability.* (1) This section applies to each covered aircraft operator beginning on the date that TSA assumes the watch list matching function for the passengers and non-traveling individuals to whom that covered aircraft operator issues a boarding pass or other authorization to enter a sterile area. TSA will provide prior written notification to the covered aircraft operator no later than 60 days before the date on which it will assume the watch list matching function from that covered aircraft operator.

(2) Prior to the date that TSA assumes the watch list matching function from a covered aircraft operator, the covered aircraft operator must comply with existing watch list matching procedures for passengers and non-traveling individuals, including denial of transport or sterile area access or designation for enhanced screening for individuals identified by the covered aircraft operator or TSA.

(b) *Watch list matching results.* Except as provided in paragraph (b) of this section, a covered aircraft operator must not issue a boarding pass or other authorization to enter a sterile area to a passenger or a non-traveling individual, and must not allow that individual to board an aircraft or enter a sterile area, until TSA informs the covered aircraft operator of the results of watch list matching for that passenger or non-traveling individual, in response to the covered aircraft operator's most recent SFPD submission for that passenger or non-traveling individual.

(1) *Denial of boarding pass.* If TSA sends a covered aircraft operator a boarding pass printing result that says the passenger or non-traveling individual must be placed on inhibited status, the covered aircraft operator must not issue a boarding pass or other authorization to enter a sterile area to that individual and must not allow that individual to board an aircraft or enter a sterile area.

(2) *Selection for enhanced screening.* If TSA sends a covered aircraft operator a boarding pass printing result that says the passenger has been selected for enhanced screening at a security checkpoint, the covered aircraft operator may issue a boarding pass to that individual and must identify the individual for enhanced screening, in accordance with procedures approved by TSA. The covered aircraft operator must place a code on the boarding pass that meets the requirements described in the Consolidated User Guide. If TSA sends a covered aircraft operator a boarding pass printing result that says the non-traveling individual has been selected for enhanced screening at a security checkpoint, the covered aircraft operator must not issue an authorization to enter a sterile area to that individual.

(3) *Cleared for boarding or entry into a sterile area.* If TSA sends a covered aircraft operator a boarding pass printing result that instructs a covered aircraft operator that a passenger or non-traveling individual is cleared, the covered aircraft operator may issue a boarding pass or other authorization to enter a sterile area to that individual, unless required under another TSA requirement to identify the passenger or non-traveling individual for enhanced screening or to deny entry into the sterile area. The covered aircraft operator must place a code on the boarding pass or authorization to enter the sterile area that meets the requirements described in the Consolidated User Guide.

(4) *Override by a covered aircraft operator.* No covered aircraft operator may override a TSA boarding pass printing result that instructs a covered aircraft operator to place a passenger or non-traveling individual in an inhibited status or to identify a passenger or non-traveling individual for enhanced screening, unless explicitly authorized by TSA to do so.

(5) *Updated SFPD from covered aircraft operator.* When a covered aircraft operator sends updated SFPD to TSA under §1560.101(d) for a passenger or non-traveling individual for whom TSA has already issued a boarding pass printing result, all previous TSA results concerning the passenger or non-traveling individual are voided. The covered aircraft operator may not issue a boarding pass or grant authorization to enter a sterile area until it receives an updated result from TSA authorizing the issuance of a boarding pass or authorization to enter a sterile area. Upon receiving an updated result from TSA, the covered aircraft operator must acknowledge receipt of the updated result, comply with the updated result, and disregard all previous boarding pass printing results.

(6) *Updated boarding pass printing results from TSA.* After TSA sends a covered aircraft operator a result under paragraph (b)(1), (b)(2), or (b)(3) of this section, TSA may receive additional information concerning the passenger or non-traveling individual and may send an updated boarding pass printing result concerning that passenger or non-traveling individual to the covered aircraft operator. Upon receiving an updated boarding pass printing result from TSA, the covered aircraft operator must acknowledge receipt of the updated result, comply with the updated result, and disregard all previous results.

(7) *Boarding pass issuance for covered flights to or overflying the United States.* Covered aircraft operators may permit another aircraft operator to issue a boarding pass for a covered flight departing from a foreign location to the United States or overflying the United States without regard to the requirements in paragraphs (b)(1) through (b)(6) of this section provided that—

(i) Before allowing the individual to board the aircraft for a covered flight, the covered aircraft operator confirms that it has received a boarding pass printing result from DHS for individuals who are issued boarding passes under paragraph (b)(7) of this section;

(ii) Before allowing the individual to board an aircraft for a covered flight, the covered aircraft operator applies the measures in its security program to prevent an individual for whom DHS has returned an inhibited status boarding pass printing result under paragraph (b)(1) of this section from boarding the aircraft; and

(iii) The covered aircraft operator applies the measures in its security program, as provided in 49 CFR part 1544,

subpart B or 49 CFR part 1546, subpart B, to ensure that an individual for whom DHS returns a Selectee result under paragraph (b)(2) of this section undergoes enhanced screening pursuant to the covered aircraft operator's security program prior to that individual boarding the aircraft.

(c) *Request for identification*—(1) *In general*. If TSA has not informed the covered aircraft operator of the results of watch list matching for an individual by the time the individual attempts to check in, or informs the covered aircraft operator that an individual has been placed in inhibited status, the aircraft operator must request from the individual a verifying identity document pursuant to procedures in its security program., as provided in 49 CFR part 1544, subpart B or 49 CFR part 1546, subpart B. The individual must present a verifying identity document to the covered aircraft operator at the airport.

(2) *Transmission of Updated Secure Flight Passenger Data*. Upon reviewing a passenger's verifying identity document, the covered aircraft operator must transmit the SFPD elements from the individual's verifying identity document to TSA.

(3) *Provision of Passenger Resolution Information*. If requested by TSA, the covered aircraft operator must also provide to TSA the individual's Passenger Resolution Information as specified by TSA.

(4) *Exception for minors*. If a covered aircraft operator is required to obtain information from an individual's verifying identity document under this paragraph (c), and the individual is younger than 18 years of age and does not have a verifying identity document, TSA may, on a case-by-case basis, authorize the minor or an adult accompanying the minor to state the individual's full name and date of birth in lieu of providing a verifying identity document.

(d) *Failure to obtain identification*. If a passenger or non-traveling individual does not present a verifying identity document when requested by the covered aircraft operator, in order to comply with paragraph (c) of this section, the covered aircraft operator must not issue a boarding pass or give authorization to enter a sterile area to that individual and must not allow that individual to board an aircraft or enter a sterile area, unless otherwise authorized by TSA.

§ 1560.107 Use of watch list matching results by covered aircraft operators.

A covered aircraft operator must not use any watch list matching results provided by TSA for purposes other than those provided in § 1560.105 and other security purposes.

§ 1560.109 Aircraft Operator Implementation Plan.

(a) *Content of the Aircraft Operator Implementation Plan (AOIP)*. Each covered aircraft operator must adopt and carry out an AOIP that sets forth the following:

(1) The covered aircraft operator's test plan with TSA.

(2) When the covered operator will begin to collect and transmit to TSA each data element of the SFPD for each covered flight.

(3) The specific means by which the covered aircraft operator will request and transmit information under § 1560.101, the timing and frequency of transmission, and any other related matters, in accordance with the Consolidated User Guide.

(b) *Adoption of Aircraft Operator Implementation Plan (AOIP)*. Each covered aircraft operator must adopt an AOIP pursuant to the procedures set forth in this paragraph (b).

(1) TSA notifies each covered aircraft operator in writing of a proposed AOIP, fixing a period of not less than 30 days within which the covered aircraft operator may submit written information, views, and arguments on the proposed AOIP.

(2) After considering all relevant material, TSA's designated official notifies each covered aircraft operator of its AOIP. The AOIP becomes effective not less than 30 days after the covered aircraft operator receives the notice of its AOIP, unless the covered aircraft operator petitions the Assistant Secretary or designated official to reconsider no later than 15 days before the effective date of the AOIP. The covered

aircraft operator must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the AOIP.

(3) Upon receipt of a petition for reconsideration, the designated official either amends the AOIP or transmits the petition, together with any pertinent information, to the Assistant Secretary or designee for reconsideration. The Assistant Secretary or designee disposes of the petition within 30 days of receipt by either directing the designated official to withdraw or amend the AOIP, or by affirming the AOIP.

(4) TSA may, at its discretion, grant extensions to any schedule deadlines, on its own initiative or upon the request of a covered aircraft operator.

(c) *Incorporation into Security Program.* Once an AOIP is approved, the AOIP becomes part of the covered aircraft operator's security program as described in 49 CFR part 1544, subpart B, or 49 CFR part 1546, subpart B, as appropriate, and any amendments will be made in accordance with the procedures in those subparts.

(d) *Handling of Aircraft Operator Implementation Plan (AOIP).* An AOIP contains sensitive security information (SSI) and must be handled and protected in accordance with 49 CFR part 1520.

§ 1560.111 Covered airport operators.

(a) *Applicability.* This section applies to a covered airport operator that has a program approved by TSA through which the covered airport operator may authorize non-traveling individuals to enter a sterile area.

(b) *Requirements.* A covered airport operator must adopt and carry out an AOIP in accordance with §1560.109. Each covered airport operator must comply with the procedures required of covered aircraft operators in §§1560.101(a), (c), and (d), 1560.103, and 1560.107 of this part and any other applicable TSA requirements when authorizing non-traveling individuals to enter a sterile area.

Subpart C—Passenger Redress

§ 1560.201 Applicability.

This subpart applies to individuals who believe they have been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of the Secure Flight program.

§ 1560.203 Representation by counsel.

A person may be represented by counsel at his or her own expense during the redress process.

§ 1560.205 Redress process.

(a) If an individual believes he or she has been improperly or unfairly delayed or prohibited from boarding an aircraft or entering a sterile area as a result of the Secure Flight program, the individual may seek assistance through the redress process established under this section.

(b) An individual may obtain the forms and information necessary to initiate the redress process on the DHS TRIP Web site at *http://www.dhs.gov/trip* or by contacting the DHS TRIP office by mail. Individuals should send written requests for forms to the DHS TRIP office and include their name and address in the request. DHS will provide the necessary forms and information to individuals through its Web site or by mail.

(c) The individual must send to the DHS TRIP office the personal information and copies of the specified identification documents. If TSA needs additional information in order to continue the redress process, TSA will so notify the individual in writing and request that additional information. The DHS TRIP Office will assign the passenger a unique identifier, which TSA will recognize as the Redress Number, and the passenger may use that Redress Number in future correspondence with TSA and when making future travel reservations.

(d) TSA, in coordination with the TSC and other appropriate Federal law enforcement or intelligence agencies, if necessary, will review all the documentation and information requested

from the individual, correct any erroneous information, and provide the individual with a timely written response.

§ 1560.207 Oversight of process.

The redress process and its implementation are subject to review by the TSA and DHS Privacy Offices and the TSA and DHS Offices for Civil Rights and Civil Liberties.

PART 1562—OPERATIONS IN THE WASHINGTON, DC, METROPOLITAN AREA

Subpart A—Maryland Three Airports: Enhanced Security Procedures for Operations at Certain Airports in the Washington, DC, Metropolitan Area Flight Restricted Zone

Subpart B—Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations

AUTHORITY: 49 U.S.C. 114, 40114, Sec. 823, Pub. L. 108–176, 117 Stat. 2595.

SOURCE: 70 FR 7162, Feb. 10, 2005, unless otherwise noted.

Subpart A—Maryland Three Airports: Enhanced Security Procedures for Operations at Certain Airports in the Washington, DC, Metropolitan Area Flight Restricted Zone

§ 1562.1 Scope and definitions.

(a) *Scope.* This subpart applies to the following airports, and individuals who operate an aircraft to or from those airports, that are located within the airspace designated as the Washington, DC, Metropolitan Area Flight Restricted Zone by the Federal Aviation Administration:

(1) College Park Airport (CGS);

(2) Potomac Airfield (VKX); and

(3) Washington Executive/Hyde Field (W32).

(b) *Definitions.* For purposes of this section:

Airport security coordinator means the official at a Maryland Three Airport who is responsible for ensuring that the airport's security procedures are implemented and followed.

Maryland Three Airport means any of the airports specified in paragraph (a) of this section.

§ 1562.3 Operating requirements.

(a) *Airport operator requirements.* Each operator of a Maryland Three Airport must:

(1) Appoint an airport employee as the airport security coordinator;

(2) Maintain and carry out security procedures approved by TSA;

(3) Maintain at the airport a copy of the airport's TSA-approved security procedures;

(4) Maintain at the airport a copy of each Federal Aviation Administration Notice to Airmen and rule that affects security procedures at the Maryland Three Airports; and

(5) Permit officials authorized by TSA to inspect—

(i) The airport;

(ii) The airport's TSA-approved security procedures; and

(iii) Any other documents required under this section.

(b) *Airport security coordinator requirements.* Each airport security coordinator for a Maryland Three Airport must be approved by TSA. To obtain TSA approval, an airport security coordinator must:

(1) Present to TSA, in a form and manner acceptable to TSA, his or her—

(i) Name;

(ii) Social Security Number;

(iii) Date of birth;

(iv) Address;

(v) Phone number; and

(vi) Fingerprints.

(2) Successfully complete a TSA terrorist threat assessment; and

(3) Not have been convicted or found not guilty by reason of insanity, in any jurisdiction, during the 10 years prior

to applying for authorization to operate to or from the airport, or while authorized to operate to or from the airport, of any crime specified in 49 CFR 1542.209 or 1572.103.

(c) *Security procedures.* To be approved by TSA, an airport's security procedures, at a minimum, must:

(1) Identify and provide contact information for the airport's airport security coordinator.

(2) Contain a current record of the individuals and aircraft authorized to operate to or from the airport.

(3) Contain procedures to—

(i) Monitor the security of aircraft at the airport during operational and non-operational hours; and

(ii) Alert the aircraft owner(s) and operator(s), the airport operator, and TSA of unsecured aircraft.

(4) Contain procedures to implement and maintain security awareness procedures at the airport.

(5) Contain procedures for limited approval of pilots who violate the Washington, DC, Metropolitan Area Flight Restricted Zone and are forced to land at the airport.

(6) Contain any additional procedures required by TSA to provide for the security of aircraft operations to or from the airport.

(d) *Amendments to security procedures.* Airport security procedures approved by TSA remain in effect unless TSA determines that—

(1) Operations at the airport have not been conducted in accordance with those procedures; or

(2) The procedures must be amended to provide for the security of aircraft operations to or from the airport.

(e) *Pilot requirements for TSA approval.* Except as specified in paragraph (g) of this section, each pilot of an aircraft operating to or from any of the Maryland Three Airports must be approved by TSA. To obtain TSA approval, a pilot must:

(1) Present to TSA—

(i) The pilot's name;

(ii) The pilot's Social Security Number;

(iii) The pilot's date of birth;

(iv) The pilot's address;

(v) The pilot's phone number;

(vi) The pilot's current and valid airman certificate or current student pilot certificate;

(vii) The pilot's current medical certificate;

(viii) One form of Government-issued picture identification of the pilot;

(ix) The pilot's fingerprints, in a form and manner acceptable to TSA; and

(x) A list containing the make, model, and registration number of each aircraft that the pilot intends to operate to or from the airport.

(2) Successfully complete a TSA terrorist threat assessment.

(3) Receive a briefing acceptable to TSA and the Federal Aviation Administration that describes procedures for operating to and from the airport.

(4) Not have been convicted or found not guilty by reason of insanity, in any jurisdiction, during the 10 years prior to applying for authorization to operate to or from the airport, or while authorized to operate to or from the airport, of any crime specified in 49 CFR 1542.209 or 1572.103.

(5) Not, in TSA's discretion, have a record on file with the Federal Aviation Administration of a violation of—

(i) A prohibited area designated under 14 CFR part 73;

(ii) A flight restriction established under 14 CFR 91.141;

(iii) Special security instructions issued under 14 CFR 99.7;

(iv) A restricted area designated under 14 CFR part 73;

(v) Emergency air traffic rules issued under 14 CFR 91.139;

(vi) A temporary flight restriction designated under 14 CFR 91.137, 91.138, or 91.145; or

(vii) An area designated under 14 CFR 91.143.

(f) *Additional pilot requirements.* Except as specified in paragraph (g) of this section, each pilot of an aircraft operating to or from any of the Maryland Three Airports must:

(1) Protect from unauthorized disclosure any identification information issued by TSA or the Federal Aviation Administration for the conduct of operations to or from the airport.

(2) Secure the aircraft after returning to the airport from any flight.

(3) Comply with any other requirements for operating to or from the airport specified by TSA or the Federal Aviation Administration.

(g) *Operations to any of the Maryland Three Airports.* A pilot who is approved by TSA in accordance with paragraph (d) of this section may operate an aircraft to any of the Maryland Three Airports, provided that the pilot—

(1) Files an instrument flight rules or visual flight rules flight plan with Leesburg Automated Flight Service Station;

(2) Obtains an Air Traffic Control clearance with a discrete transponder code; and

(3) Follows any arrival/departure procedures required by the Federal Aviation Administration.

(h) *U.S. Armed forces, law enforcement, and aeromedical services aircraft.* An individual may operate a U.S. Armed Forces, law enforcement, or aeromedical services aircraft on an authorized mission to or from any of the Maryland Three Airports provided that the individual complies with any requirements for operating to or from the airport specified by TSA or the Federal Aviation Administration.

(i) *Continuing responsibilities.* (1) If an airport security coordinator, or a pilot who is approved to operate to or from any of the Maryland Three Airports, is convicted or found not guilty by reason of insanity, in any jurisdiction, of any crime specified in 49 CFR 1542.209 or 1572.103, the airport security coordinator or pilot must notify TSA within 24 hours of the conviction or finding of not guilty by reason of insanity. TSA may withdraw its approval of the airport security coordinator or pilot as a result of the conviction or finding of not guilty by reason of insanity.

(2) If a pilot who is approved to operate to or from any of the Maryland Three Airports commits any of the violations described in paragraph (e)(5) of this section, the pilot must notify TSA within 24 hours of the violation. TSA, in its discretion, may withdraw its approval of the pilot as a result of the violation.

(3) If an airport security coordinator, or a pilot who is approved to operate to or from any of the Maryland Three Airports, is determined by TSA to pose a threat to national or transportation security, or a threat of terrorism, TSA may withdraw its approval of the airport security coordinator or pilot.

(j) *Waivers.* TSA, in coordination with the Federal Aviation Administration, the United States Secret Service, and any other relevant agency, may permit an operation to or from any of the Maryland Three Airports, in deviation from the provisions of this section, if TSA finds that such action—

(1) Is in the public interest; and

(2) Provides the level of security required by this section.

Subpart B—Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations

SOURCE: 70 FR 41600, July 19, 2005, unless otherwise noted.

§ 1562.21 Scope, general requirements, and definitions.

(a) *Scope.* This subpart applies to aircraft operations into or out of Ronald Reagan Washington National Airport (DCA), fixed base operators located at DCA or gateway airports; individuals designated as a security coordinator by aircraft operators or fixed base operators; and crewmembers, passengers, and armed security officers on aircraft operations subject to this subpart.

(b) *General requirements.* Each person operating an aircraft into or out of DCA must comply with this subpart, except:

(1) Military, law enforcement, and medivac aircraft operations;

(2) Federal and State government aircraft operations operating under an airspace waiver approved by TSA and the Federal Aviation Administration;

(3) All-cargo aircraft operations; and

(4) Passenger aircraft operations conducted under:

(i) A full security program approved by TSA in accordance with 49 CFR 1544.101(a); or

(ii) A foreign air carrier security program approved by TSA in accordance with 49 CFR 1546.101(a) or (b).

(c) *Other security programs.* Each aircraft operator required to comply with this subpart for an aircraft operation into or out of DCA must also comply

with any other TSA-approved security program that covers that operation. If any requirements of the DASSP conflict with the requirements of another TSA-approved security program, the aircraft operation must be conducted in accordance with the requirements of the DASSP.

(d) *Definitions.* For purposes of this subpart, the following definitions apply:

Armed Security Officer Program means the security program approved by TSA, in coordination with the Federal Air Marshal Service, for security officers authorized to carry a firearm under §1562.29 of this part.

Crewmember means a person assigned to perform duty in an aircraft during flight time. This does not include an armed security officer.

DCA means Ronald Reagan Washington National Airport.

DASSP means the aircraft operator security program (DCA Access Standard Security Program) approved by TSA under this part for aircraft operations into and out of DCA.

FBO means a fixed base operator that has been approved by TSA under this part to serve as a last point of departure for flights into or out of DCA.

FBO Security Program means the security program approved by TSA under this part for FBOs to serve flights into or out of DCA.

Flightcrew member means a pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time.

Gateway airport means an airport that has been approved by TSA under this part as a last point of departure for flights into DCA under this part.

Passenger means any person on an aircraft other than a flightcrew member. A ''passenger'' includes an armed security officer authorized to carry a firearm in accordance with the rule.

§1562.23 Aircraft operator and passenger requirements.

(a) *General.* To operate into or out of DCA, an aircraft operator must:

(1) Designate a security coordinator responsible for implementing the DASSP and other security requirements required under this section, and provide TSA with the security coordinator's contact information and availability in accordance with the DASSP.

(2) Adopt and carry out the DASSP.

(3) Ensure that each crewmember of an aircraft operating into or out of DCA meets the requirements of paragraph (c) of this section.

(4) Apply for and receive a reservation from the Federal Aviation Administration and authorization from TSA for each flight into and out of DCA in accordance with paragraph (d) of this section.

(5) Comply with the operating requirements in paragraph (e) of this section for each flight into and out of DCA.

(6) Pay any costs and fees required under this part.

(7) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know, and refer all requests for SSI by other persons to TSA.

(8) Comply with any additional security procedures required by TSA through order, Security Directive, or other means.

(b) *Security coordinator.* Each security coordinator designated by an aircraft operator under paragraph (a) of this section:

(1) Must undergo a fingerprint-based criminal history records check that does not disclose that he or she has a disqualifying criminal offense as described in §1544.229(d) of this chapter. This standard is met if the security coordinator is in compliance with the fingerprint-based criminal history records check requirements of §§1542.209, 1544.229, or 1544.230 of this chapter with his or her current employer.

(2) Must submit to TSA his or her:

(i) Legal name, including first, middle, and last; any applicable suffix, and any other names used.

(ii) Current mailing address, including residential address if different than current mailing address.

(iii) Date and place of birth.

(iv) Social security number, (submission is voluntary, although recommended).

(v) Citizenship status and date of naturalization if the individual is a naturalized citizen of the United States.

(vi) Alien registration number, if applicable.

(3) Must successfully complete a TSA security threat assessment.

(4) May, if informed that a disqualifying offense has been disclosed, correct the record in accordance with the procedures set forth in paragraphs (h) and (i) of §1544.229 of this chapter regarding notification and correction of records.

(c) *Flightcrew member requirements.* Each flightcrew member of an aircraft, as defined in 49 CFR 1540.5, operating into or out of DCA:

(1) Must undergo a fingerprint-based criminal history records check that does not disclose that he or she has a disqualifying criminal offense as described in §1544.229(d) of this chapter. This standard is met if the flightcrew member is in compliance with the fingerprint-based criminal history records check requirements of §§1542.209, 1544.229, or 1544.230 of this chapter with his or her current employer.

(2) Must not have a record on file with the Federal Aviation Administration of a violation of—

(i) A prohibited area designated under 14 CFR part 73;

(ii) A flight restriction established under 14 CFR 91.141;

(iii) Special security instructions issued under 14 CFR 99.7;

(iv) A restricted area designated under 14 CFR part 73;

(v) Emergency air traffic rules issued under 14 CFR 91.139;

(vi) A temporary flight restriction designated under 14 CFR 91.137, 91.138, or 91.145; or

(vii) An area designated under 14 CFR 91.143.

(3) May, if informed that a disqualifying offense has been disclosed, correct the record in accordance with the procedures set forth in paragraphs (h) and (i) of §1544.229 of this chapter regarding notification and correction of records.

(d) *Flight authorization requirements.* To receive authorization to operate an aircraft into or out of DCA, an aircraft operator must follow the procedures in this paragraph.

(1) The aircraft operator must apply to the Federal Aviation Administration for a tentative reservation, in a form and manner approved by the Federal Aviation Administration.

(2) The aircraft operator must submit to TSA, in a form and manner approved by TSA, the following information at least 24 hours prior to aircraft departure:

(i) For each passenger and crewmember on the aircraft:

(A) Legal name, including first, middle, and last; any applicable suffix, and any other names used.

(B) Current mailing address, including residential address if different than current mailing address.

(C) Date and place of birth.

(D) Social security number, (submission is voluntary, although recommended).

(E) Citizenship status and date of naturalization if the individual is a naturalized citizen of the United States.

(F) Alien registration number, if applicable.

(ii) The registration number of the aircraft.

(iii) The flight plan.

(iv) Any other information required by TSA.

(3) TSA will conduct a name-based security threat assessment for each passenger and crewmember. If TSA notifies the aircraft operator that a passenger or crewmember may pose a security threat, the aircraft operator must ensure that the passenger or crewmember does not board the aircraft before the aircraft departs out of DCA or out of a gateway airport to DCA.

(4) If TSA approves the flight, TSA will transmit such approval to the Federal Aviation Administration for assignment of a final reservation to operate into or out of DCA. Once the Federal Aviation Administration assigns the final reservation, TSA will notify the aircraft operator.

(5) TSA may, at its discretion, cancel any or all flight approvals at any time without prior notice to the aircraft operator.

(6) TSA may, at its discretion, permit a flight into or out of DCA to deviate from the requirements of this subpart, if TSA finds that such action would not

be detrimental to transportation security or the safe operation of the aircraft.

(7) TSA may, at its discretion, require any flight into or out of DCA under this subpart to comply with additional security measures.

(e) *Operating requirements.* Each aircraft operator must:

(1) Ensure that each flight into DCA departs from a gateway airport and makes no intermediate stops before arrival at DCA.

(2) Ensure that each passenger and crewmember on an aircraft operating into or out of DCA has been screened in accordance with the DASSP prior to boarding the aircraft.

(3) Ensure that all accessible property and property in inaccessible cargo holds on an aircraft operating into or out of DCA has been screened in accordance with the DASSP prior to boarding the aircraft.

(4) Ensure that each aircraft operating into or out of DCA has been searched in accordance with the DASSP.

(5) Ensure that each passenger and crewmember on an aircraft operating into or out of DCA provides TSA with a valid government-issued picture identification in accordance with the DASSP.

(6) If the aircraft operating into or out of DCA is equipped with a cockpit door, ensure that the door is closed and locked at all times during the operation of the aircraft to or from DCA, unless Federal Aviation Administration regulations require the door to remain open.

(7) Ensure that each aircraft operating into or out of DCA has onboard at least one armed security officer who meets the requirements of §1562.29 of this chapter. This requirement does not apply if—

(i) There is a Federal Air Marshal onboard; or

(ii) The aircraft is being flown without passengers into DCA to pick up passengers, or out of DCA after deplaning all passengers.

(8) Ensure that an aircraft operating into or out of DCA has any Federal Air Marshal onboard, at no cost to the Federal Government, if TSA or the Federal Air Marshal Service so requires.

(9) Notify the National Capital Region Coordination Center prior to departure of the aircraft from DCA or a gateway airport.

(10) Ensure that each aircraft operating into or out of DCA operates under instrument flight rules.

(11) Ensure that each passenger complies with any security measures mandated by TSA.

(12) Ensure that no prohibited items are onboard the aircraft.

(f) *Compliance.* (1) Each aircraft operator must:

(i) Permit TSA to conduct any inspections or tests, including copying records, to determine compliance with this part and the DASSP.

(ii) At the request of TSA, provide evidence of compliance with this part and the DASSP, including copies of records.

(2) Noncompliance with this part or the DASSP may result in the cancellation of an aircraft operator's flight approvals and other remedial or enforcement action, as appropriate.

(g) *Passenger requirements.* Each passenger, including each armed security officer, who boards or attempts to board an aircraft under this section must:

(1) Provide information to the aircraft operator as provided in this section.

(2) Provide to TSA upon request a valid government-issued photo identification.

(3) Comply with security measures as conveyed by the aircraft operator.

(4) Comply with all applicable regulations in this chapter, including §1540.107 regarding submission to screening and inspection, §1540.109 regarding prohibition against interference with screening personnel, and §1540.111 regarding carriage of weapons, explosives, and incendiaries by individuals.

§1562.25 Fixed base operator requirements.

(a) *Security program.* Each FBO must adopt and carry out an FBO Security Program.

(b) *Screening and other duties.* Each FBO must—

(1) Designate a security coordinator who meets the requirements in

§ 1562.23(b) of this part and is responsible for implementing the FBO Security Program and other security requirements required under this section, and provide TSA with the security coordinator's contact information and availability in accordance with the FBO Security Program.

(2) Support the screening of persons and property in accordance with the requirements of this subpart and the FBO Security Program.

(3) Support the search of aircraft in accordance with the requirements of this subpart and the FBO Security Program.

(4) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know, and refer all requests for SSI by other persons to TSA.

(5) Perform any other duties required under the FBO Security Program.

(c) *Compliance.* (1) Each FBO must:

(i) Permit TSA to conduct any inspections or tests, including copying records, to determine compliance with this part and the FBO Security Program.

(ii) At the request of TSA, provide evidence of compliance with this part and the FBO Security Program, including copies of records.

(2) Noncompliance with this part or the FBO Security Program may result in the cancellation of an aircraft operator's flight approvals and other remedial or enforcement action, as appropriate.

§ 1562.27 Costs.

(a) Each aircraft operator must pay a threat assessment fee of $15 for each passenger and crewmember whose information the aircraft operator submits to TSA in accordance with § 1562.23(d) of this part.

(b) Each aircraft operator must pay to TSA the costs associated with carrying out this subpart, as provided in its DASSP.

(c) All fees and reimbursement must be remitted to TSA in a form and manner approved by TSA.

(d) TSA will not issue any refunds, unless any fees or reimbursement funds were paid in error.

(e) If an aircraft operator does not remit to TSA the fees and reimbursement funds required under this section, TSA may decline to process any requests for authorization from the aircraft operator.

§ 1562.29 Armed security officer requirements.

(a) *General.* Unless otherwise authorized by TSA, each armed security officer must meet the following requirements:

(1) Be qualified to carry a firearm in accordance with paragraph (b) of this section.

(2) Successfully complete a TSA security threat assessment as described in paragraph (c) of this section.

(3) Meet such other requirements as TSA, in coordination with the Federal Air Marshal Service, may establish in the Armed Security Officer Security Program.

(4) Be authorized by TSA, in coordination with the Federal Air Marshal Service, under 49 U.S.C. 44903(d).

(b) *Qualifications.* To be qualified to carry a firearm under this subpart, an individual must meet the requirements in paragraph (1), (2), or (3) of this section, unless otherwise authorized by TSA, in coordination with the Federal Air Marshal Service.

(1) *Active law enforcement officers.* An active law enforcement officer must be an employee of a governmental agency who—

(i) Is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law;

(ii) Has statutory powers of arrest;

(iii) Is authorized by the agency to carry a firearm;

(iv) Is not the subject of any disciplinary action by the agency;

(v) Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(vi) Is not prohibited by Federal law from receiving a firearm.

(2) *Retired law enforcement officers.* A retired law enforcement officer must be an individual who—

(i) Retired in good standing from service with a public agency as a law

enforcement officer, other than for reasons of mental instability;

(ii) Before such retirement, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest;

(iii) Before such retirement, was regularly employed as a law enforcement officer for an aggregate of 15 years or more, or retired from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by such agency;

(iv) Has a non-forfeitable right to benefits under the retirement plan of the agency;

(v) Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(vi) Is not prohibited by Federal law from receiving a firearm.

(3) *Other individuals.* Any other individual must—

(i) Meet qualifications established by TSA, in coordination with the Federal Air Marshal Service, in the Armed Security Officer Program;

(ii) Not be under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(iii) Not be prohibited by Federal law from receiving a firearm.

(c) *Threat assessments.* To be authorized under this section, each armed security officer:

(1) Must undergo a fingerprint-based criminal history records check that does not disclose that he or she has a criminal offense that would disqualify him or her from possessing a firearm under 18 U.S.C. 922(g).

(2) May, if informed that a disqualifying offense has been disclosed, correct the record in accordance with the procedures set forth in paragraphs (h) and (i) of §1544.229 of this chapter regarding notification and correction of records.

(3) Must submit to TSA his or her:

(i) Legal name, including first, middle, and last; any applicable suffix, and any other names used.

(ii) Current mailing address, including residential address if different than current mailing address.

(iii) Date and place of birth.

(iv) Social security number, (submission is voluntary, although recommended).

(v) Citizenship status and date of naturalization if the individual is a naturalized citizen of the United States.

(vi) Alien registration number, if applicable.

(4) Must undergo a threat assessment by TSA prior to receiving authorization under this section and prior to boarding an aircraft operating into or out of DCA as provided in §1562.23(d)(1) of this part.

(d) *Training.* Each armed security officer onboard an aircraft operating into or out of DCA must:

(1) Have basic law enforcement training acceptable to TSA; and

(2) Successfully complete a TSA-approved training course, developed in coordination with the Federal Air Marshal Service, at the expense of the armed security officer.

(e) *Armed security officer program.* (1) Each armed security officer onboard an aircraft operating into or out of DCA must—

(i) Comply with the Armed Security Officer Program.

(ii) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know, and refer all requests for SSI by other persons to TSA.

(2) TSA and the Federal Air Marshal Service may conduct random inspections of armed security officers to ensure compliance with the Armed Security Officer Program.

(f) *Authority to carry firearm.* An armed security officer approved under this section is authorized—

(1) To carry a firearm in accordance with the Armed Security Officer Program on an aircraft operating under a DASSP into or out of DCA; and

(2) To transport a firearm in accordance with the Armed Security Officer Program at any airport as needed to carry out duties under this subpart, including for travel to and from flights conducted under this subpart.

(g) *Use of force.* Each armed security officer authorized to carry a firearm under this section may use force, including deadly force, in accordance

with the Armed Security Officer Program.

(h) *Use of alcohol or intoxicating or hallucinatory drugs or substances.* An armed security officer onboard an aircraft operating into or out of DCA may not consume alcohol or use an intoxicating or hallucinatory drug or substance during the flight and within 8 hours before boarding the aircraft.

(i) *Credential*—(1) *TSA credential.* An armed security officer under this section must carry a credential issued by TSA.

(2) *Inspection of credential.* An armed security officer must present the TSA-issued credential for inspection when requested by an authorized representative of TSA, the Federal Aviation Administration, the Federal Air Marshal Service, the National Transportation Safety Board, any Federal, State, or local law enforcement officer, or any authorized aircraft operator representative.

(3) *Preflight identification to crewmembers.* When carrying a firearm, an armed security officer must identify himself or herself to all crewmembers either personally or through another member of the crew before the flight.

(j) *Suspension or withdrawal of authorization.* At the discretion of TSA, authorization under this subpart and 49 U.S.C. 44903(d) is suspended or withdrawn upon notification by TSA.

SUBCHAPTER D—MARITIME AND LAND TRANSPORTATION SECURITY

PART 1570—GENERAL RULES

Sec.

AUTHORITY: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469; Pub. L. 110–53 secs. 1414, 1522.

SOURCE: 72 FR 3593, Jan. 25, 2007, unless otherwise noted.

§ 1570.1 Scope.

This part applies to any person involved in land or maritime transportation as specified in this subchapter.

§ 1570.3 Terms used in this subchapter.

For purposes of this subchapter:

Adjudicate means to make an administrative determination of whether an applicant meets the standards in this subchapter, based on the merits of the issues raised.

Alien means any person not a citizen or national of the United States.

Alien registration number means the number issued by the U.S. Department of Homeland Security to an individual when he or she becomes a lawful permanent resident of the United States or attains other lawful, non-citizen status.

Applicant means a person who has applied for one of the security threat assessments identified in this subchapter.

Assistant Administrator for Threat Assessment and Credentialing (Assistant Administrator) means the officer designated by the Assistant Secretary to administer the appeal and waiver programs described in this part, except where the Assistant Secretary is specifically designated in this part to administer the appeal or waiver program. The Assistant Administrator may appoint a designee to assume his or her duties.

Assistant Secretary means Assistant Secretary for Homeland Security, Transportation Security Administration (Assistant Secretary), the highest ranking TSA official, or his or her designee, and who is responsible for making the final determination on the appeal of an intelligence-related check under this part.

Commercial drivers license (CDL) is used as defined in 49 CFR 383.5.

Convicted means any plea of guilty or nolo contendere, or any finding of guilt, except when the finding of guilt is subsequently overturned on appeal, pardoned, or expunged. For purposes of this subchapter, a conviction is expunged when the conviction is removed from the individual's criminal history record and there are no legal disabilities or restrictions associated with the expunged conviction, other than the fact that the conviction may be used for sentencing purposes for subsequent convictions. In addition, where an individual is allowed to withdraw an original plea of guilty or nolo contendere and enter a plea of not guilty and the case is subsequently dismissed, the individual is no longer considered to have a conviction for purposes of this subchapter.

Determination of No Security Threat means an administrative determination by TSA that an individual does not pose a security threat warranting denial of an HME or a TWIC.

Federal Maritime Security Coordinator (FMSC) has the same meaning as defined in 46 U.S.C. 70103(a)(2)(G); is the Captain of the Port (COTP) exercising authority for the COTP zones described in 33 CFR part 3, and is the Port Facility Security Officer as described in the International Ship and Port Facility Security (ISPS) Code, part A.

Final Determination of Threat Assessment means a final administrative determination by TSA, including the resolution of related appeals, that an individual poses a security threat warranting denial of an HME or a TWIC.

Hazardous materials endorsement (HME) means the authorization for an individual to transport hazardous materials in commerce, an indication of which must be on the individual's commercial driver's license, as provided in the Federal Motor Carrier Safety Administration (FMCSA) regulations in 49 CFR part 383.

Imprisoned or imprisonment means confined to a prison, jail, or institution for the criminally insane, on a full-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity. Time spent confined or restricted to a half-way house, treatment facility, or similar institution, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity, does not constitute imprisonment for purposes of this rule.

Incarceration means confined or otherwise restricted to a jail-type institution, half-way house, treatment facility, or another institution, on a full or part-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity.

Initial Determination of Threat Assessment means an initial administrative determination by TSA that an applicant poses a security threat warranting denial of an HME or a TWIC.

Initial Determination of Threat Assessment and Immediate Revocation means an initial administrative determination that an individual poses a security threat that warrants immediate revocation of an HME or invalidation of a TWIC. In the case of an HME, the State must immediately revoke the HME if TSA issues an Initial Determination of Threat Assessment and Immediate Revocation. In the case of a TWIC, TSA invalidates the TWIC when TSA issues an Initial Determination of Threat Assessment and Immediate Revocation.

Invalidate means the action TSA takes to make a credential inoperative when it is reported as lost, stolen, damaged, no longer needed, or when TSA determines an applicant does not meet the security threat assessment standards of 49 CFR part 1572.

Lawful permanent resident means an alien lawfully admitted for permanent residence, as defined in 8 U.S.C. 1101(a)(20).

Maritime facility has the same meaning as ''facility'' together with ''OCS facility'' (Outer Continental Shelf facility), as defined in 33 CFR 101.105.

Mental health facility means a mental institution, mental hospital, sanitarium, psychiatric facility, and any other facility that provides diagnoses by licensed professionals of mental retardation or mental illness, including a psychiatric ward in a general hospital.

National of the United States means a citizen of the United States, or a person who, though not a citizen, owes permanent allegiance to the United States, as defined in 8 U.S.C. 1101(a)(22), and includes American Samoa and Swains Island.

Owner/operator with respect to a maritime facility or a vessel has the same meaning as defined in 33 CFR 101.105.

Revocation means the termination, deactivation, rescission, invalidation, cancellation, or withdrawal of the privileges and duties conferred by an HME or TWIC, when TSA determines an applicant does not meet the security threat assessment standards of 49 CFR part 1572.

Secure area means the area on board a vessel or at a facility or outer continental shelf facility, over which the owner/operator has implemented security measures for access control, as defined by a Coast Guard approved security plan. It does not include passenger access areas or public access areas, as those terms are defined in 33 CFR 104.106 and 105.106 respectively. Vessels operating under the waivers provided for at 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. Facilities subject to 33 CFR chapter I, subchapter H, part 105 may, with approval of the Coast Guard, designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure areas.

Security threat means an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism.

Sensitive security information (SSI) means information that is described in,

and must be managed in accordance with, 49 CFR part 1520.

State means a State of the United States and the District of Columbia.

Transportation Worker Identification Credential (TWIC) means a Federal biometric credential, issued to an individual, when TSA determines that the individual does not pose a security threat.

Withdrawal of Initial Determination of Threat Assessment is the document that TSA issues after issuing an Initial Determination of Security Threat, when TSA determines that an individual does not pose a security threat that warrants denial of an HME or TWIC.

[72 FR 3593, Jan. 25, 2007; 72 FR 14050, Mar. 26, 2007]

§ 1570.5 Fraud and intentional falsification of records.

No person may make, cause to be made, attempt, or cause to attempt any of the following:

(a) Any fraudulent or intentionally false statement in any record or report that is kept, made, or used to show compliance with the subchapter, or exercise any privileges under this subchapter.

(b) Any reproduction or alteration, for fraudulent purpose, of any record, report, security program, access medium, or identification medium issued under this subchapter or pursuant to standards in this subchapter.

§ 1570.7 Fraudulent use or manufacture; responsibilities of persons.

(a) No person may use or attempt to use a credential, security threat assessment, access control medium, or identification medium issued or conducted under this subchapter that was issued or conducted for another person.

(b) No person may make, produce, use or attempt to use a false or fraudulently created access control medium, identification medium or security threat assessment issued or conducted under this subchapter.

(c) No person may tamper or interfere with, compromise, modify, attempt to circumvent, or circumvent TWIC access control procedures.

(d) No person may cause or attempt to cause another person to violate paragraphs (a)–(c) of this section.

§ 1570.9 Inspection of credential.

(a) Each person who has been issued or possesses a TWIC must present the TWIC for inspection upon a request from TSA, the Coast Guard, or other authorized DHS representative; an authorized representative of the National Transportation Safety Board; or a Federal, State, or local law enforcement officer.

(b) Each person who has been issued or who possesses a TWIC must allow his or her TWIC to be read by a reader and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a PIN, to the reader, upon a request from TSA, the Coast Guard, other authorized DHS representative; or a Federal, State, or local law enforcement officer.

§ 1570.11 Compliance, inspection, and enforcement.

(a) Each owner/operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an owner/operator with—

(1) This subchapter and part 1520 of this chapter; and

(2) 46 U.S.C. 70105 and 49 U.S.C. 114.

(b) At the request of TSA, each owner/operator must provide evidence of compliance with this subchapter and part 1520 of this chapter, including copies of records.

§ 1570.13 False statements regarding security background checks by public transportation agency or railroad carrier.

(a) *Scope.* This section implements sections 1414(e) (6 U.S.C. 1143) and 1522(e) (6 U.S.C. 1170) of the ''Implementing Recommendations of the 9/11 Commission Act of 2007,'' Pub. L. 110–53.

(b) *Definitions.*

Covered individual means an employee of a public transportation agency or a contractor or subcontractor of a public transportation agency or an employee of a railroad carrier or a contractor or subcontractor of a railroad carrier.

Public transportation agency means a publicly-owned operator of public

transportation eligible to receive Federal assistance under chapter 53 of title 49, United States Code.

Railroad has the meaning that term has in section 20102 of title 49, United States Code.

Railroad carrier has the meaning that term has in section 20102 of title 49, United States Code.

Security background check means reviewing the following for the purpose of identifying individuals who may pose a threat to transportation security, national security, or of terrorism:

(i) Relevant criminal history databases;

(ii) In the case of an alien (as defined in sec. 101 of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)), the relevant databases to determine the status of the alien under the immigration laws of the United States; and

(iii) Other relevant information or databases, as determined by the Secretary of Homeland Security.

(c) *Prohibitions.* (1) A public transportation agency or a contractor or subcontractor of a public transportation agency may not knowingly misrepresent to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary of Homeland Security related to security background check requirements for covered individuals when conducting a security background check.

(2) A railroad carrier or a contractor or subcontractor of a railroad carrier may not knowingly misrepresent to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary of Homeland Security related to security background check requirements for covered individuals when conducting a security background check.

[73 FR 44669, July 31, 2008]

PART 1572—CREDENTIALING AND SECURITY THREAT ASSESSMENTS

Subpart A—Procedures and General Standards

Subpart B—Qualification Standards for Security Threat Assessments

Subpart C—Transportation of Hazardous Materials From Canada or Mexico To and Within the United States by Land Modes

Subpart D [Reserved]

Subpart E—Fees for Security Threat Assessments for Hazmat Drivers

AUTHORITY: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

SOURCE: 72 FR 3595, Jan. 25, 2007, unless otherwise noted.

Subpart A—Procedures and General Standards

§ 1572.1 Applicability.

This part establishes regulations for credentialing and security threat assessments for certain maritime and land transportation workers.

§ 1572.3 Scope.

This part applies to—

(a) State agencies responsible for issuing a hazardous materials endorsement (HME); and

(b) An applicant who—

(1) Is qualified to hold a commercial driver's license under 49 CFR parts 383 and 384, and is applying to obtain, renew, or transfer an HME; or

(2) Is applying to obtain or renew a TWIC in accordance with 33 CFR parts 104 through 106 or 46 CFR part 10; is a commercial driver licensed in Canada or Mexico and is applying for a TWIC to transport hazardous materials in accordance with 49 CFR 1572.201; or other individuals approved by TSA.

[72 FR 3595, Jan. 25, 2007, as amended at 72 FR 55048, Sept. 28, 2007]

§ 1572.5 Standards for security threat assessments.

(a) *Standards.* TSA determines that an applicant poses a security threat warranting denial of an HME or TWIC, if—

(1) The applicant has a disqualifying criminal offense described in 49 CFR 1572.103;

(2) The applicant does not meet the immigration status requirements described in 49 CFR 1572.105;

(3) TSA conducts the analyses described in 49 CFR 1572.107 and determines that the applicant poses a security threat; or

(4) The applicant has been adjudicated as lacking mental capacity or committed to a mental health facility, as described in 49 CFR 1572.109.

(b) *Immediate Revocation/Invalidation.* TSA may invalidate a TWIC or direct a State to revoke an HME immediately, if TSA determines during the security threat assessment that an applicant poses an immediate threat to transportation security, national security, or of terrorism.

(c) *Violation of FMCSA Standards.* The regulations of the Federal Motor Carrier Safety Administration (FMCSA) provide that an applicant is disqualified from operating a commercial motor vehicle for specified periods, if he or she has an offense that is listed in the FMCSA rules at 49 CFR 383.51. If records indicate that an applicant has committed an offense that would disqualify the applicant from operating a commercial motor vehicle under 49 CFR 383.51, TSA will not issue a Determination of No Security Threat until the State or the FMCSA determine that the applicant is not disqualified under that section.

(d) *Waiver.* In accordance with the requirements of §1515.7, applicants may apply for a waiver of certain security threat assessment standards.

(e) *Comparability of Other Security Threat Assessment Standards.* TSA may determine that security threat assessments conducted by other governmental agencies are comparable to the threat assessment described in this part, which TSA conducts for HME and TWIC applicants.

(1) In making a comparability determination, TSA will consider—

(i) The minimum standards used for the security threat assessment;

(ii) The frequency of the threat assessment;

(iii) The date of the most recent threat assessment; and

(iv) Whether the threat assessment includes biometric identification and a biometric credential.

(2) To apply for a comparability determination, the agency seeking the determination must contact the Assistant Program Manager, Attn: Federal Agency Comparability Check, Hazmat

Threat Assessment Program, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202–4220.

(3) TSA will notify the public when a comparability determination is made.

(4) An applicant, who has completed a security threat assessment that is determined to be comparable under this section to the threat assessment described in this part, must complete the enrollment process and provide biometric information to obtain a TWIC, if the applicant seeks unescorted access to a secure area of a vessel or facility. The applicant must pay the fee listed in 49 CFR 1572.503 for information collection/credential issuance.

(5) TSA has determined that the security threat assessment for an HME under this part is comparable to the security threat assessment for TWIC.

(6) TSA has determined that the security threat assessment for a FAST card, under the Free and Secure Trade program administered by U.S. Customs and Border Protection, is comparable to the security threat assessment described in this part.

§ 1572.7 [Reserved]

§ 1572.9 Applicant information required for HME security threat assessment.

An applicant must supply the information required in this section, in a form acceptable to TSA, when applying to obtain or renew an HME. When applying to transfer an HME from one State to another, 49 CFR 1572.13(e) applies.

(a) Except as provided in (a)(12) through (16), the applicant must provide the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current and previous mailing address, current residential address if it differs from the current mailing address, and e-mail address if available. If the applicant prefers to receive correspondence and notification via e-mail, the applicant should so state.

(3) Date of birth.

(4) Gender.

(5) Height, weight, hair color, and eye color.

(6) City, state, and country of birth.

(7) Immigration status and, if the applicant is a naturalized citizen of the United States, the date of naturalization.

(8) Alien registration number, if applicable.

(9) The State of application, CDL number, and type of HME(s) held.

(10) Name, telephone number, facsimile number, and address of the applicant's current employer(s), if the applicant's work for the employer(s) requires an HME. If the applicant's current employer is the U.S. military service, include branch of the service.

(11) Whether the applicant is applying to obtain, renew, or transfer an HME or for a waiver.

(12) Social security number. Providing the social security number is voluntary; however, failure to provide it will delay and may prevent completion of the threat assessment.

(13) Passport number. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(14) Department of State Consular Report of Birth Abroad. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(15) Whether the applicant has previously completed a TSA threat assessment, and if so the date and program for which it was completed. This information is voluntary and may expedite the adjudication process for applicants who have completed a TSA security threat assessment.

(16) Whether the applicant currently holds a federal security clearance, and if so, the date of and agency for which the clearance was performed. This information is voluntary and may expedite the adjudication process for applicants who have completed a federal security threat assessment.

(b) The applicant must provide a statement, signature, and date of signature that he or she—

(1) Was not convicted, or found not guilty by reason of insanity, of a disqualifying crime listed in 49 CFR 1572.103(b), in a civilian or military jurisdiction, during the seven years before the date of the application, or is applying for a waiver;

(2) Was not released from incarceration, in a civilian or military jurisdiction, for committing a disqualifying crime listed in 49 CFR 1572.103(b), during the five years before the date of the application, or is applying for a waiver;

(3) Is not wanted, or under indictment, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103, or is applying for a waiver;

(4) Was not convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense identified in 49 CFR 1572.103(a), in a civilian or military jurisdiction, or is applying for a waiver;

(5) Has not been adjudicated as lacking mental capacity or committed to a mental health facility involuntarily or is applying for a waiver;

(6) Meets the immigration status requirements described in 49 CFR 1572.105;

(7) Has or has not served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations, under 49 CFR 1572.11, impose a continuing obligation on the HME holder to disclose to the State if he or she is convicted, or found not guilty by reason of insanity, of a disqualifying crime, adjudicated as lacking mental capacity, or committed to a mental health facility.

(c) The applicant must certify and date receipt the following statement:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 5103a. Purpose: This information is needed to verify your identity and to conduct a security threat assessment to evaluate your suitability for a hazardous materials endorsement for a commercial driver's license. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will delay and may prevent completion of your security threat assessment. Routine Uses: Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

(d) The applicant must certify and date receipt the following statement, immediately before the signature line:

The information I have provided on this application is true, complete, and correct, to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact on this application can be punished by fine or imprisonment or both (*See* section 1001 of Title 18 United States Code), and may be grounds for denial of a hazardous materials endorsement.

(e) The applicant must certify the following statement in writing:

I acknowledge that if the Transportation Security Administration determines that I pose a security threat, my employer, as listed on this application, may be notified. If TSA or other law enforcement agency becomes aware of an imminent threat to a maritime facility or vessel, TSA may provide limited information necessary to reduce the risk of injury or damage to the facility or vessel.

§ 1572.11 Applicant responsibilities for HME security threat assessment.

(a) *Surrender of HME.* If an individual is disqualified from holding an HME under 49 CFR 1572.5(c), he or she must surrender the HME to the licensing State. Failure to surrender the HME to the State may result in immediate revocation under 49 CFR 1572.13(a) and/or civil penalties.

(b) *Continuing responsibilities.* An individual who holds an HME must surrender the HME as required in paragraph (a) of this section within 24 hours, if the individual—

(1) Is convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103; or

(2) Is adjudicated as lacking mental capacity, or committed to a mental health facility, as described in 49 CFR 1572.109; or

(3) Renounces or loses U.S. citizenship or status as a lawful permanent resident; or

(4) Violates his or her immigration status, and/or is ordered removed from the United States.

(c) *Submission of fingerprints and information.* (1) An HME applicant must submit fingerprints and the information required in 49 CFR 1572.9, in a form acceptable to TSA, when so notified by the State, or when the applicant applies to obtain or renew an HME. The procedures outlined in 49 CFR 1572.13(e) apply to HME transfers.

(2) When submitting fingerprints and the information required in 49 CFR 1572.9, the fee described in 49 CFR 1572.503 must be remitted to TSA.

§ 1572.13 State responsibilities for issuance of hazardous materials endorsement.

Each State must revoke an individual's HME immediately, if TSA informs the State that the individual does not meet the standards for security threat assessment in 49 CFR 1572.5 and issues an Initial Determination of Threat Assessment and Immediate Revocation.

(a) No State may issue or renew an HME for a CDL, unless the State receives a Determination of No Security Threat from TSA.

(b) Each State must notify each individual holding an HME issued by that State that he or she will be subject to the security threat assessment described in this part as part of an application for renewal of the HME, at least 60 days prior to the expiration date of the individual's HME. The notice must inform the individual that he or she may initiate the security threat assessment required by this section at any time after receiving the notice, but no later than 60 days before the expiration date of the individual's HME.

(c) The State that issued an HME may extend the expiration date of the HME for 90 days, if TSA has not provided a Determination of No Security Threat or a Final Determination of Threat Assessment before the expiration date. Any additional extension must be approved in advance by TSA.

(d) Within 15 days of receipt of a Determination of No Security Threat or Final Determination of Threat Assessment from TSA, the State must—

(1) Update the applicant's permanent record to reflect:

(i) The results of the security threat assessment;

(ii) The issuance or denial of an HME; and

(iii) The new expiration date of the HME.

(2) Notify the Commercial Drivers License Information System (CDLIS) operator of the results of the security threat assessment.

(3) Revoke or deny the applicant's HME if TSA serves the State with a Final Determination of Threat Assessment.

(e) For applicants who apply to transfer an existing HME from one State to another, the second State will not require the applicant to undergo a new security threat assessment until the security threat assessment renewal period established in the preceding issuing State, not to exceed five years, expires.

(f) A State that is not using TSA's agent to conduct enrollment for the security threat assessment must retain the application and information required in 49 CFR 1572.9, for at least one year, in paper or electronic form.

§ 1572.15 Procedures for HME security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA completes includes a fingerprint-based criminal history records check (CHRC), an intelligence-related background check, and a final disposition.

(b) *Fingerprint-based check.* In order to conduct a fingerprint-based CHRC, the following procedures must be completed:

(1) The State notifies the applicant that he or she will be subject to the security threat assessment at least 60 days prior to the expiration of the applicant's HME, and that the applicant must begin the security threat assessment no later than 30 days before the date of the expiration of the HME.

(2) Where the State elects to collect fingerprints and applicant information, the State—

(i) Collects fingerprints and applicant information required in 49 CFR 1572.9;

(ii) Provides the applicant information to TSA electronically, unless otherwise authorized by TSA;

(iii) Transmits the fingerprints to the FBI/Criminal Justice Information Services (CJIS), in accordance with the

FBI/CJIS fingerprint submission standards; and

(iv) Retains the signed application, in paper or electronic form, for one year and provides it to TSA, if requested.

(3) Where the State elects to have a TSA agent collect fingerprints and applicant information—

(i) TSA provides a copy of the signed application to the State;

(ii) The State retains the signed application, in paper or electronic form, for one year and provides it to TSA, if requested; and

(iii) TSA transmits the fingerprints to the FBI/CJIS, in accordance with the FBI/CJIS fingerprint submission standards.

(4) TSA receives the results from the FBI/CJIS and adjudicates the results of the check, in accordance with 49 CFR 1572.103 and, if applicable, 49 CFR 1572.107.

(c) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1572.9.

(2) Searches domestic and international Government databases described in 49 CFR 1572.105, 1572.107, and 1572.109.

(3) Adjudicates the results of the check in accordance with 49 CFR 1572.103, 1572.105, 1572.107, and 1572.109.

(d) *Final disposition.* Following completion of the procedures described in paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the State in which the applicant is authorized to hold an HME, if TSA determines that an applicant meets the security threat assessment standards described in 49 CFR 1572.5.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant, if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting denial of the HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5 or 1515.9, as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant, the applicant's employer where appropriate, and the State, if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5 and may pose an imminent threat to transportation or national security, or of terrorism. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting immediate revocation of an HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5(h) or 1515.9(f), as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination and Immediate Revocation, the Initial Determination and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) If the applicant does not appeal the Initial Determination of Threat Assessment or Initial Determination of Threat Assessment and Immediate Revocation, TSA serves a Final Determination of Threat Assessment on the State in which the applicant applied for the HME, the applicant's employer where appropriate, and on the applicant, if the appeal of the Initial Determination results in a finding that the applicant poses a security threat.

(5) If the applicant appeals the Initial Determination of Threat Assessment

or the Initial Determination of Threat Assessment and Immediate Revocation, the procedures in 49 CFR 1515.5 or 1515.9 apply.

(6) Applicants who do not meet certain standards in 49 CFR 1572.103, 1572.105, or 1572.109 may seek a waiver in accordance with 49 CFR 1515.7.

§ 1572.17 Applicant information required for TWIC security threat assessment.

An applicant must supply the information required in this section, in a form acceptable to TSA, when applying to obtain or renew a TWIC.

(a) Except as provided in (a)(12) through (16), the applicant must provide the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current and previous mailing address, current residential address if it differs from the current mailing address, and e-mail address if available. If the applicant wishes to receive notification that the TWIC is ready to be retrieved from the enrollment center via telephone rather than e-mail address, the applicant should state this and provide the correct telephone number.

(3) Date of birth.

(4) Gender.

(5) Height, weight, hair color, and eye color.

(6) City, state, and country of birth.

(7) Immigration status, and

(i) If the applicant is a naturalized citizen of the United States, the date of naturalization;

(ii) If the applicant is present in the United States based on a Visa, the type of Visa, the Visa number, and the date on which it expires; and

(iii) If the applicant is a commercial driver licensed in Canada and does not hold a FAST card, a Canadian passport.

(8) If not a national or citizen of the United States, the alien registration number and/or the number assigned to the applicant on the U.S. Customs and Border Protection Arrival-Departure Record, Form I–94.

(9) Except as described in paragraph (a)(9)(i) of this section, the reason that the applicant requires a TWIC, including, as applicable, the applicant's job description and the primary facility, vessel, or maritime port location(s) where the applicant will most likely require unescorted access, if known. This statement does not limit access to other facilities, vessels, or ports, but establishes eligibility for a TWIC.

(i) Applicants who are commercial drivers licensed in Canada or Mexico who are applying for a TWIC in order to transport hazardous materials in accordance with 49 CFR 1572.201 and not to access secure areas of a facility or vessel, must explain this in response to the information requested in paragraph (a)(9) of this section.

(10) The name, telephone number, and address of the applicant's current employer(s), if working for the employer requires a TWIC. If the applicant's current employer is the U.S. military service, include the branch of the service. An applicant whose current employer does not require possession of a TWIC, does not have a single employer, or is self-employed, must provide the primary vessel or port location(s) where the applicant requires unescorted access, if known. This statement does not limit access to other facilities, vessels, or ports, but establishes eligibility for a TWIC.

(11) If a credentialed mariner or applying to become a credentialed mariner, proof of citizenship as required in 46 CFR chapter I, subchapter B.

(12) Social security number. Providing the social security number is voluntary; however, failure to provide it will delay and may prevent completion of the threat assessment.

(13) Passport number, city of issuance, date of issuance, and date of expiration. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(14) Department of State Consular Report of Birth Abroad. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(15) Whether the applicant has previously completed a TSA threat assessment, and if so the date and program for which it was completed. This information is voluntary and may expedite the adjudication process for applicants

who have completed a TSA security threat assessment.

(16) Whether the applicant currently holds a federal security clearance, and if so, the date of and agency for which the clearance was performed. This information is voluntary and may expedite the adjudication process for applicants who have completed a federal security threat assessment.

(b) The applicant must provide a statement, signature, and date of signature that he or she—

(1) Was not convicted, or found not guilty by reason of insanity, of a disqualifying crime listed in 49 CFR 1572.103(b), in a civilian or military jurisdiction, during the seven years before the date of the application, or is applying for a waiver;

(2) Was not released from incarceration, in a civilian or military jurisdiction, for committing a disqualifying crime listed in 49 CFR 1572.103(b), during the five years before the date of the application, or is applying for a waiver;

(3) Is not wanted, or under indictment, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103, or is applying for a waiver;

(4) Was not convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense identified in 49 CFR 1572.103(a), in a civilian or military jurisdiction, or is applying for a waiver;

(5) Has not been adjudicated as lacking mental capacity, or committed to a mental health facility involuntarily, or is applying for a waiver;

(6) Meets the immigration status requirements described in 49 CFR 1572.105;

(7) Has, or has not, served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations under 49 CFR 1572.19 impose a continuing obligation on the TWIC holder to disclose to TSA if he or she is convicted, or found not guilty by reason of insanity, of a disqualifying crime, adjudicated as lacking mental capacity, or committed to a mental health facility.

(c) Applicants, applying to obtain or renew a TWIC, must submit biometric information to be used for identity verification purposes. If an individual cannot provide the selected biometric, TSA will collect an alternative biometric identifier.

(d) The applicant must certify and date receipt the following statement:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 5103a. Purpose: This information is needed to verify your identity and to conduct a security threat assessment to evaluate your suitability for a Transportation Worker Identification Credential. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will delay and may prevent completion of your security threat assessment. Routine Uses: Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

(e) The applicant must certify the following statement in writing:

As part of my employment duties, I am required to have unescorted access to secure areas of maritime facilities or vessels in which a Transportation Worker Identification Credential is required; I am now, or I am applying to be, a credentialed merchant mariner; or I am a commercial driver licensed in Canada or Mexico transporting hazardous materials in accordance with 49 CFR 1572.201.

(f) The applicant must certify and date receipt the following statement, immediately before the signature line:

The information I have provided on this application is true, complete, and correct, to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact on this application, can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of a Transportation Worker Identification Credential.

(g) The applicant must certify the following statement in writing:

I acknowledge that if the Transportation Security Administration determines that I

pose a security threat, my employer, as listed on this application, may be notified. If TSA or other law enforcement agency becomes aware of an imminent threat to a maritime facility or vessel, TSA may provide limited information necessary to reduce the risk of injury or damage to the facility or vessel.

§ 1572.19 Applicant responsibilities for a TWIC security threat assessment.

(a) *Implementation schedule.* Except as provided in paragraph (b) of this section, applicants must provide the information required in 49 CFR 1572.17, when so directed by the owner/operator.

(b) *Implementation schedule for certain mariners.* An applicant, who holds a Merchant Mariner Document (MMD) issued after February 3, 2003, and before April 15, 2009, or a Merchant Marine License (License) issued after January 13, 2006, and before April 15, 2009, must submit the information required in this section, but is not required to undergo the security threat assessment described in this part.

(c) *Surrender of TWIC.* The TWIC is property of the Transportation Security Administration. If an individual is disqualified from holding a TWIC under 49 CFR 1572.5, he or she must surrender the TWIC to TSA. Failure to surrender the TWIC to TSA may result in immediate revocation under 49 CFR 1572.5(b) and/or civil penalties.

(d) *Continuing responsibilities.* An individual who holds a TWIC must surrender the TWIC, as required in paragraph (a) of this section, within 24 hours if the individual—

(1) Is convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103; or

(2) Is adjudicated as lacking mental capacity or committed to a mental health facility, as described in 49 CFR 1572.109; or

(3) Renounces or loses U.S. citizenship or status as a lawful permanent resident; or

(4) Violates his or her immigration status and/or is ordered removed from the United States.

(e) *Submission of fingerprints and information.* (1) TWIC applicants must submit fingerprints and the information required in 49 CFR 1572.17, in a form acceptable to TSA, to obtain or renew a TWIC.

(2) When submitting fingerprints and the information required in 49 CFR 1572.17, the fee required in 49 CFR 1572.503 must be remitted to TSA.

(f) *Lost, damaged, or stolen credentials.* If an individual's TWIC is damaged, or if a TWIC holder loses possession of his or her credential, he or she must notify TSA immediately.

[72 FR 3595, Jan. 25, 2007, as amended at 72 FR 55048, Sept. 28, 2007; 73 FR 25566, May 7, 2008]

§ 1572.21 Procedures for TWIC security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA conducts includes a fingerprint-based criminal history records check (CHRC), an intelligence-related check, and a final disposition.

(b) *Fingerprint-based check.* The following procedures must be completed to conduct a fingerprint-based CHRC:

(1) Consistent with the implementation schedule described in 49 CFR 1572.19(a) and (b), and as required in 33 CFR 104.200, 105.200, or 106.200, applicants are notified.

(2) During enrollment, TSA—

(i) Collects fingerprints, applicant information, and the fee required in 49 CFR 1572.17;

(ii) Transmits the fingerprints to the FBI/CJIS in accordance with the FBI/CJIS fingerprint submission standards.

(iii) Receives and adjudicates the results of the check from FBI/CJIS, in accordance with 49 CFR 1572.103 and, if applicable, 49 CFR 1572.107.

(c) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1572.17;

(2) Searches domestic and international Government databases required to determine if the applicant meets the requirements of 49 CFR 1572.105, 1572.107, and 1572.109;

(3) Adjudicates the results of the check in accordance with 49 CFR 1572.103, 1572.105, 1572.107, and 1572.109.

(d) *Final disposition.* Following completion of the procedures described in

paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the applicant if TSA determines that the applicant meets the security threat assessment standards described in 49 CFR 1572.5. In the case of a mariner, TSA also serves a Determination of No Security Threat on the Coast Guard.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting denial of the TWIC;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5 or 1515.9, as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant, the applicant's employer where appropriate, the FMSC, and in the case of a mariner applying for a TWIC, on the Coast Guard, if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5 and may pose an imminent security threat. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting immediate revocation of a TWIC and unescorted access to secure areas;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5(h) or 1515.9(f), as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination and Immediate Revocation, the Initial Determination and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) If the applicant does not appeal the Initial Determination of Threat Assessment or Initial Determination of Threat Assessment and Immediate Revocation, TSA serves a Final Determination of Threat Assessment on the FMSC and in the case of a mariner, on the Coast Guard, and the applicant's employer where appropriate.

(5) If the applicant appeals the Initial Determination of Threat Assessment or the Initial Determination of Threat Assessment and Immediate Revocation, the procedures in 49 CFR 1515.5 or 1515.9 apply.

(6) Applicants who do not meet certain standards in 49 CFR 1572.103, 1572.105, or 1572.109 may seek a waiver in accordance with 49 CFR 1515.7.

§ 1572.23 TWIC expiration.

(a) A TWIC expires five years after the date it was issued at the end of the calendar day, except as follows:

(1) The TWIC was issued based on a determination that the applicant completed a comparable threat assessment. If issued pursuant to a comparable threat assessment, the TWIC expires five years from the date on the credential associated with the comparable threat assessment.

(2) The applicant is in a lawful nonimmigrant status category listed in 1572.105(a)(7), and the status expires, the employer terminates the employment relationship with the applicant, or the applicant otherwise ceases working for the employer. Under any of these circumstances, TSA deems the TWIC to have expired regardless of the expiration date on the face of the TWIC.

(b) TSA may issue a TWIC for a term less than five years to match the expiration of a visa.

§§ 1572.24—1572.40 [Reserved]

Subpart B—Standards for Security Threat Assessments

§ 1572.101 Scope.

This subpart applies to applicants who hold or are applying to obtain or renew an HME or TWIC, or transfer an HME. Applicants for an HME also are subject to safety requirements issued by the Federal Motor Carrier Safety Administration under 49 CFR part 383 and by the State issuing the HME, including additional immigration status and criminal history standards.

§ 1572.103 Disqualifying criminal offenses.

(a) *Permanent disqualifying criminal offenses.* An applicant has a permanent disqualifying offense if convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following felonies:

(1) Espionage or conspiracy to commit espionage.

(2) Sedition, or conspiracy to commit sedition.

(3) Treason, or conspiracy to commit treason.

(4) A federal crime of terrorism as defined in 18 U.S.C. 2332b(g), or comparable State law, or conspiracy to commit such crime.

(5) A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. 70101. The term ''economic disruption'' does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute.

(6) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a State law that is comparable.

(7) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).

(8) Murder.

(9) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.

(10) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, *et seq.*, or a comparable State law, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the crimes listed in paragraph (a) of this section.

(11) Attempt to commit the crimes in paragraphs (a)(1) through (a)(4).

(12) Conspiracy or attempt to commit the crimes in paragraphs (a)(5) through (a)(10).

(b) *Interim disqualifying criminal offenses.* (1) The felonies listed in paragraphs (b)(2) of this section are disqualifying, if either:

(i) the applicant was convicted, or found not guilty by reason of insanity, of the crime in a civilian or military jurisdiction, within seven years of the date of the application; or

(ii) the applicant was incarcerated for that crime and released from incarceration within five years of the date of the TWIC application.

(2) The interim disqualifying felonies are:

(i) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.

(ii) Extortion.

(iii) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering is related to a crime described in paragraphs (a) or (b) of this section. Welfare fraud and passing bad

checks do not constitute dishonesty, fraud, or misrepresentation for purposes of this paragraph.

(iv) Bribery.

(v) Smuggling.

(vi) Immigration violations.

(vii) Distribution of, possession with intent to distribute, or importation of a controlled substance.

(viii) Arson.

(ix) Kidnapping or hostage taking.

(x) Rape or aggravated sexual abuse.

(xi) Assault with intent to kill.

(xii) Robbery.

(xiii) Fraudulent entry into a seaport as described in 18 U.S.C. 1036, or a comparable State law.

(xiv) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, *et seq.*, or a comparable State law, other than the violations listed in paragraph (a)(10) of this section.

(xv) Conspiracy or attempt to commit the crimes in this paragraph (b).

(c) *Under want, warrant, or indictment.* An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in this section, is disqualified until the want or warrant is released or the indictment is dismissed.

(d) *Determination of arrest status.* (1) When a fingerprint-based check discloses an arrest for a disqualifying crime listed in this section without indicating a disposition, TSA will so notify the applicant and provide instructions on how the applicant must clear the disposition, in accordance with paragraph (d)(2) of this section.

(2) The applicant must provide TSA with written proof that the arrest did not result in conviction for the disqualifying criminal offense, within 60 days after the service date of the notification in paragraph (d)(1) of this section. If TSA does not receive proof in that time, TSA will notify the applicant that he or she is disqualified. In the case of an HME, TSA will notify the State that the applicant is disqualified, and in the case of a mariner applying for TWIC, TSA will notify the Coast Guard that the applicant is disqualified.

[72 FR 3595, Jan. 25, 2007; 72 FR 5633, Feb. 7, 2007; 72 FR 14050, Mar. 26, 2007]

§ 1572.105 Immigration status.

(a) An individual applying for a security threat assessment for a TWIC or HME must be a national of the United States or—

(1) A lawful permanent resident of the United States;

(2) A refugee admitted under 8 U.S.C. 1157;

(3) An alien granted asylum under 8 U.S.C. 1158;

(4) An alien in valid M–1 nonimmigrant status who is enrolled in the United States Merchant Marine Academy or a comparable State maritime academy. Such individuals may serve as unlicensed mariners on a documented vessel, regardless of their nationality, under 46 U.S.C. 8103.

(5) A nonimmigrant alien admitted under the Compact of Free Association between the United States and the Federated States of Micronesia, the United States and the Republic of the Marshall Islands, or the United States and Palau.

(6) An alien in lawful nonimmigrant status who has unrestricted authorization to work in the United States, except—

(i) An alien in valid S–5 (informant of criminal organization information) lawful nonimmigrant status;

(ii) An alien in valid S–6 (informant of terrorism information) lawful nonimmigrant status;

(iii) An alien in valid K–1 (Fianco(e)) lawful nonimmigrant status; or

(iv) An alien in valid K–2 (Minor child of Fianco(e)) lawful nonimmigrant status.

(7) An alien in the following lawful nonimmigrant status who has restricted authorization to work in the United States—

(i) B1/OCS Business Visitor/Outer Continental Shelf;

(ii) C–1/D Crewman Visa;

(iii) H–1B Special Occupations;

(iv) H–1B1 Free Trade Agreement;

(v) E–1 Treaty Trader;

(vi) E–3 Australian in Specialty Occupation;

(vii) L–1 Intracompany Executive Transfer;

(viii) O–1 Extraordinary Ability;

(ix) TN North American Free Trade Agreement;

(x) E–2 Treaty Investor; or

(xi) Another authorization that confers legal status, when TSA determines that the legal status is comparable to the legal status set out in paragraph (a)(7) of this section.

(8) A commercial driver licensed in Canada or Mexico who is admitted to the United States under 8 CFR 214.2(b)(4)(i)(E) to conduct business in the United States.

(b) Upon expiration of a nonimmigrant status listed in paragraph (a)(7) of this section, an employer must retrieve the TWIC from the applicant and provide it to TSA.

(c) Upon expiration of a nonimmigrant status listed in paragraph (a)(7) of this section, an employee must surrender his or her TWIC to the employer.

(d) If an employer terminates an applicant working under a nonimmigrant status listed in paragraph (a)(7) of this section, or the applicant otherwise ceases working for the employer, the employer must notify TSA within 5 business days and provide the TWIC to TSA if possible.

(e) Any individual in removal proceedings or subject to an order of removal under the immigration laws of the United States is not eligible to apply for a TWIC.

(f) To determine an applicant's immigration status, TSA will check relevant Federal databases and may perform other checks, including the validity of the applicant's alien registration number, social security number, or I–94 Arrival-Departure Form number.

[72 FR 3595, Jan. 25, 2007, as amended at 72 FR 55049, Sept. 28, 2007; 73 FR 13156, Mar. 12, 2008]

§ 1572.107 Other analyses.

(a) TSA may determine that an applicant poses a security threat based on a search of the following databases:

(1) Interpol and other international databases, as appropriate.

(2) Terrorist watchlists and related databases.

(3) Any other databases relevant to determining whether an applicant poses, or is suspected of posing, a security threat, or that confirm an applicant's identity.

(b) TSA may also determine that an applicant poses a security threat, if the search conducted under this part reveals extensive foreign or domestic criminal convictions, a conviction for a serious crime not listed in 49 CFR 1572.103, or a period of foreign or domestic imprisonment that exceeds 365 consecutive days.

§ 1572.109 Mental capacity.

(a) An applicant has mental incapacity, if he or she has been—

(1) Adjudicated as lacking mental capacity; or

(2) Committed to a mental health facility.

(b) An applicant is adjudicated as lacking mental capacity if—

(1) A court, board, commission, or other lawful authority has determined that the applicant, as a result of marked subnormal intelligence, mental illness, incompetence, condition, or disease, is a danger to himself or herself or to others, or lacks the mental capacity to conduct or manage his or her own affairs.

(2) This includes a finding of insanity by a court in a criminal case and a finding of incompetence to stand trial; or a finding of not guilty by reason of lack of mental responsibility, by any court, or pursuant to articles 50a and 76b of the Uniform Code of Military Justice (10 U.S.C. 850a and 876b).

(c) An applicant is committed to a mental health facility if he or she is formally committed to a mental health facility by a court, board, commission, or other lawful authority, including involuntary commitment and commitment for lacking mental capacity, mental illness, and drug use. This does not include commitment to a mental health facility for observation or voluntary admission to a mental health facility.

§§ 1572.111–1572.139 [Reserved]

Subpart C—Transportation of Hazardous Materials From Canada or Mexico To and Within the United States by Land Modes

§ 1572.201 Transportation of hazardous materials via commercial motor vehicle from Canada or Mexico to and within the United States.

(a) *Applicability*. This section applies to commercial motor vehicle drivers licensed by Canada and Mexico.

(b) *Terms used in this section*. The terms used in 49 CFR parts 1500, 1570, and 1572 also apply in this subpart. In addition, the following terms are used in this subpart for purposes of this section:

FAST means Free and Secure Trade program of the Bureau of Customs and Border Protection (CBP), a cooperative effort between CBP and the governments of Canada and Mexico to coordinate processes for the clearance of commercial shipments at the border.

Hazardous materials means material that has been designated as hazardous under 49 U.S.C. 5103 and is required to be placarded under subpart F of 49 CFR part 172 or any quantity of material that listed as a select agent or toxin in 42 CFR part 73.

(c) *Background check required*. A commercial motor vehicle driver who is licensed by Canada or Mexico may not transport hazardous materials into or within the United States unless the driver has undergone a background check similar to the one required of U.S.-licensed operators with a hazardous materials endorsement (HME) on a commercial driver's license, as prescribed in 49 CFR 1572.5.

(d) *FAST card*. A commercial motor vehicle driver who holds a current Free and Secure Trade (FAST) program card satisfies the requirements of this section. Commercial motor vehicle drivers who wish to apply for a FAST program card must contact the FAST Commercial Driver Program, Bureau of Customs and Border Protection (CBP), Department of Homeland Security.

(e) *TWIC*. A commercial motor vehicle driver who holds a TWIC satisfies the requirements of this section. Commercial vehicle drivers who wish to apply for a TWIC must comply with the rules in 49 CFR part 1572.

§ 1572.203 Transportation of explosives from Canada to the United States via railroad carrier.

(a) *Applicability*. This section applies to railroad carriers that carry explosives from Canada to the United States, using a train crew member who is not a U.S. citizen or lawful permanent resident alien of the United States.

(b) *Terms under this section*. For purposes of this section:

Customs and Border Protection (CBP) means the Bureau of Customs and Border Protection, an agency within the U.S. Department of Homeland Security.

Explosive means a material that has been examined by the Associate Administrator for Hazardous Materials Safety, Research and Special Programs Administration, in accordance with 49 CFR 173.56, and determined to meet the definition for a Class 1 material in 49 CFR 173.50.

Known railroad carrier means a person that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known offeror means an offeror that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known train crew member means an individual used to transport explosives from Canada to the United States, who has been determined by the Governments of Canada and the United States to present no known security concern.

Lawful permanent resident alien means an alien lawfully admitted for permanent residence, as defined by 8 U.S.C. 1101(a)(20).

Offeror means the person offering a shipment to the railroad carrier for transportation from Canada to the United States, and may also be known as the ''consignor'' in Canada.

Railroad carrier means ''railroad carrier'' as defined in 49 U.S.C. 20102.

(c) *Prior approval of railroad carrier, offeror, and train crew member.* (1) No railroad carrier may transport in commerce any explosive into the United States from Canada, via a train operated by a crew member who is not a U.S. national or lawful permanent resident alien, unless the railroad carrier, offeror, and train crew member are identified on a TSA list as a known railroad carrier, known offeror, and known train crew member, respectively.

(2) The railroad carrier must ensure that it, its offeror, and each of its crew members have been determined to be a known railroad carrier, known offeror, and known train crew member, respectively. If any has not been so determined, the railroad carrier must submit the following information to Transport Canada:

(i) The railroad carrier's identification, including—

(A) Official name;

(B) Business number;

(C) Any trade names; and

(D) Address.

(ii) The following information about any offeror of explosives whose shipments it will carry:

(A) Official name.

(B) Business number.

(C) Address.

(iii) The following information about any train crew member the railroad carrier may use to transport explosives into the United States from Canada, who is neither a U.S. national nor lawful permanent resident alien:

(A) Full name.

(B) Both current and most recent prior residential addresses.

(3) Transport Canada will determine whether the railroad carrier and offeror are legitimately doing business in Canada and will also determine whether the train crew members present no known problems for purposes of this section. Transport Canada will notify TSA of these determinations by forwarding to TSA lists of known railroad carriers, offerors, and train crew members and their identifying information.

(4) TSA will update and maintain the list of known railroad carriers, offerors, and train crew members and forward the list to CBP.

(5) Once included on the list, the railroad carriers, offerors, and train crew members need not obtain prior approval for future transport of explosives under this section.

(d) *TSA checks.* TSA may periodically check the data on the railroad carriers, offerors, and train crew members to confirm their continued eligibility, and may remove from the list any that TSA determines is not known or is a threat to security.

(e) *At the border.* (1) Train crew members who are not U.S. nationals or lawful permanent resident aliens. Upon arrival at a point designated by CBP for inspection of trains crossing into the United States, the train crew members of a train transporting explosives must provide sufficient identification to CBP to enable that agency to determine if each crew member is on the list of known train crew members maintained by TSA.

(2) *Train crew members who are U.S. nationals or lawful permanent resident aliens.* If CBP cannot verify that the crew member is on the list and the crew member is a U.S. national or lawful permanent resident alien, the crew member may be cleared by CBP upon providing—

(i) A valid U.S. passport; or

(ii) One or more other document(s), including a form of U.S. Federal or state Government-issued identification with photograph, acceptable to CBP.

(3) *Compliance.* If a carrier attempts to enter the U.S. without having complied with this section, CBP will deny entry of the explosives and may take other appropriate action.

Subpart D [Reserved]

Subpart E—Fees for Security Threat Assessments for Hazmat Drivers

§ 1572.400 Scope and definitions.

(a) *Scope.* This part applies to—

(1) States that issue an HME for a commercial driver's license;

(2) Individuals who apply to obtain or renew an HME for a commercial driver's license and must undergo a security threat assessment under 49 CFR part 1572; and

(3) Entities who collect fees from such individuals on behalf of TSA.

(b) *Terms.* As used in this part:

Commercial driver's license (CDL) is used as defined in 49 CFR 383.5.

Day means calendar day.

FBI Fee means the fee required for the cost of the Federal Bureau of Investigation (FBI) to process fingerprint records.

Information Collection Fee means the fee required, in this part, for the cost of collecting and transmitting fingerprints and other applicant information under 49 CFR part 1572.

Threat Assessment Fee means the fee required, in this part, for the cost of TSA adjudicating security threat assessments, appeals, and waivers under 49 CFR part 1572.

TSA agent means an entity approved by TSA to collect and transmit fingerprints and applicant information, in accordance with 49 CFR part 1572, and fees in accordance with this part.

§ 1572.401 Fee collection options.

(a) *State collection and transmission.* If a State collects fingerprints and applicant information under 49 CFR part 1572, the State must collect and transmit to TSA the Threat Assessment Fee, in accordance with the requirements of 49 CFR 1572.403. The State also must collect and remit the FBI fee, in accordance with established procedures.

(b) *TSA agent collection and transmission.* If a TSA agent collects fingerprints and applicant information under 49 CFR part 1572, the agent must—

(1) Collect the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in accordance with procedures approved by TSA;

(2) Transmit to TSA the Threat Assessment Fee, in accordance with procedures approved by TSA; and

(3) Transmit to TSA the FBI Fee, in accordance with procedures approved by TSA and the FBI.

[72 FR 3595, Jan. 25, 2007; 72 FR 14050, Mar. 26, 2007]

§ 1572.403 Procedures for collection by States.

This section describes the procedures that a State, which collects fingerprints and applicant information under 49 CFR part 1572; and the procedures an individual who applies to obtain or renew an HME, for a CDL in that State, must follow for collection and transmission of the Threat Assessment Fee and the FBI Fee.

(a) *Imposition of fees.* (1) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment, under 49 CFR part 1572, for an individual who applies to obtain or renew an HME: $34.

(2) The following FBI Fee is required for the FBI to process fingerprint identification records and name checks required under 49 CFR part 1572: the fee collected by the FBI under Pub. L. 101–515.

(3) An individual who applies to obtain or renew an HME, or the individual's employer, must remit to the State the Threat Assessment Fee and the FBI Fee, in a form and manner approved by TSA and the State, when the individual submits the application for the HME to the State.

(b) *Collection of fees.* (1) A State must collect the Threat Assessment Fee and FBI Fee, when an individual submits an application to the State to obtain or renew an HME.

(2) Once TSA receives an application from a State for a security threat assessment under 49 CFR part 1572, the State is liable for the Threat Assessment Fee.

(3) Nothing in this subpart prevents a State from collecting any other fees that a State may impose on an individual who applies to obtain or renew an HME.

(c) *Handling of fees.* (1) A State must safeguard all Threat Assessment Fees, from the time of collection until remittance to TSA.

(2) All Threat Assessment Fees are held in trust by a State for the beneficial interest of the United States in paying for the costs of conducting the security threat assessment, required by 49 U.S.C. 5103a and 49 CFR part 1572. A State holds neither legal nor equitable interest in the Threat Assessment Fees, except for the right to retain any accrued interest on the principal amounts collected pursuant to this section.

(3) A State must account for Threat Assessment Fees separately, but may

commingle such fees with other sources of revenue.

(d) *Remittance of fees.* (1) TSA will generate and provide an invoice to a State on a monthly basis. The invoice will indicate the total fee dollars (number of applicants times the Threat Assessment Fee) that are due for the month.

(2) A State must remit to TSA full payment for the invoice, within 30 days after TSA sends the invoice.

(3) TSA accepts Threat Assessment Fees only from a State, not from an individual applicant for an HME.

(4) A State may retain any interest that accrues on the principal amounts collected between the date of collection and the date the Threat Assessment Fee is remitted to TSA, in accordance with paragraph (d)(2) of this section.

(5) A State may not retain any portion of the Threat Assessment Fee to offset the costs of collecting, handling, or remitting Threat Assessment Fees.

(6) Threat Assessment Fees, remitted to TSA by a State, must be in U.S. currency, drawn on a U.S. bank, and made payable to the ''Transportation Security Administration.''

(7) Threat Assessment Fees must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(8) TSA will not issue any refunds of Threat Assessment Fees.

(9) If a State does not remit the Threat Assessment Fees for any month, TSA may decline to process any HME applications from that State.

§ 1572.405 Procedures for collection by TSA.

This section describes the procedures that an individual, who applies to obtain or renew an HME for a CDL, must follow if a TSA agent collects and transmits the Information Collection Fee, Threat Assessment Fee, and FBI Fee.

(a) *Imposition of fees.* (1) The following Information Collection Fee is required for a TSA agent to collect and transmit fingerprints and applicant information, in accordance with 49 CFR part 1572: $38.

(2) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment, under 49 CFR part 1572, for an individual who applies to obtain or renew an HME: $34.

(3) The following FBI Fee is required for the FBI to process fingerprint identification records required under 49 CFR part 1572: The fee collected by the FBI under Pub. L. 101–515.

(4) An individual who applies to obtain or renew an HME, or the individual's employer, must remit to the TSA agent the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in a form and manner approved by TSA, when the individual submits the application required under 49 CFR part 1572.

(b) *Collection of fees.* A TSA agent will collect the fees required under this section, when an individual submits an application to the TSA agent, in accordance with 49 CFR part 1572.

(c) *Remittance of fees.* (1) Fees required under this section, which are remitted to a TSA agent, must be made in U.S. currency, drawn on a U.S. bank, and made payable to the ''Transportation Security Administration.''

(2) Fees required under this section must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(3) TSA will not issue any refunds of fees required under this section.

(4) Applications, submitted in accordance with 49 CFR part 1572, will be processed only upon receipt of all applicable fees under this section.

Subpart F—Fees for Security Threat Assessments for Transportation Worker Identification Credential (TWIC)

§ 1572.500 Scope.

(a) *Scope.* This part applies to—

(1) Individuals who apply to obtain or renew a Transportation Worker Identification Credential and must undergo a security threat assessment under 49 CFR part 1572; and

(2) Entities that collect fees from such individuals on behalf of TSA.

(b) *Terms.* As used in this part:

TSA agent means the entity approved by TSA to collect and transmit fingerprints and applicant information, and collect fees in accordance with this part.

§ 1572.501 Fee collection.

(a) *When fee must be paid.* When an applicant submits the information and fingerprints required under 49 CFR part 1572 to obtain or renew a TWIC, the fee must be remitted to TSA or its agent in accordance with the requirements of this section. Applications submitted in accordance with 49 CFR part 1572 will be processed only upon receipt of all required fees under this section.

(b) *Standard TWIC Fee.* The fee to obtain or renew a TWIC, except as provided in paragraphs (c) and (d) of this section, is made up of the total of the following segments:

(1) The Enrollment Segment covers the cost for TSA or its agent to enroll applicants. The Enrollment Segment fee is $43.25.

(2) The Full Card Production/Security Threat Assessment Segment covers the costs for TSA conduct security threat assessment and card production. The Full Card Production/Security Threat Assessment Segment fee is $72.

(3) The FBI Segment covers the cost for the FBI to process fingerprint identification records. The FBI Segment fee is the amount collected by the FBI under Pub. L. 101–515. If the FBI amends this fee, TSA or its agent will collect the amended fee.

(c) *Reduced TWIC Fee.* The fee to obtain a TWIC when the applicant has undergone a comparable threat assessment in connection with an HME, FAST card, other threat assessment deemed to be comparable under 49 CFR 1572.5(e) or holds a Merchant Mariner Document or Merchant Mariner License is made up of the total of the following segments:

(1) The Enrollment Segment covers the cost for TSA or its agent to enroll applicants. The Enrollment Segment fee is $43.25.

(2) The Reduced Card Production/Security Threat Assessment Segment covers the cost for TSA to conduct a portion of the security threat assessment and card production. The Reduced Card Production/Security Threat Assessment Segment fee is $62.

(d) *Card Replacement Fee.* The fee to replace a TWIC that has been lost, stolen, or damaged is $60.00.

(e) *Form of fee.* The TSA vendor will collect the fee required to obtain or renew a TWIC and will determine the method of acceptable payment, subject to approval by TSA.

(f) *Refunds.* TSA will not issue any refunds of fees required under this section.

(g) *Inflation adjustment.* The fees prescribed in this section, except the FBI fee, may be adjusted annually on or after October 1, 2007, by publication of an inflation adjustment. A final rule in the FEDERAL REGISTER will announce the inflation adjustment. The adjustment shall be a composite of the Federal civilian pay raise assumption and non-pay inflation factor for that fiscal year issued by the Office of Management and Budget for agency use in implementing OMB Circular A–76, weighted by the pay and non-pay proportions of total funding for that fiscal year. If Congress enacts a different Federal civilian pay raise percentage than the percentage issued by OMB for Circular A–76, the Department of Homeland Security may adjust the fees to reflect the enacted level. The required fee shall be the amount prescribed in paragraphs (a)(1)(i) and (a)(1)(ii), plus the latest inflation adjustment.

[72 FR 3595, Jan. 25, 2007, as amended at 72 FR 55049, Sept. 28, 2007]

PART 1580—RAIL TRANSPORTATION SECURITY

Subpart A—General

Subpart B—Freight Rail Including Freight Railroad Carriers, Rail Hazardous Materials Shippers, Rail Hazardous Materials Receivers, and Private Cars

AUTHORITY: 49 U.S.C. 114.

SOURCE: 73 FR 72173, Nov. 26, 2008, unless otherwise noted.

Subpart A—General

§ 1580.1 Scope.

(a) Except as provided in paragraph (b) of this section, this part includes requirements for the following persons. Appendix B of this part summarizes the general requirements for each person, and the specific sections in this part provide detailed requirements.

(1) Each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation;

(2) Each rail hazardous materials shipper that offers, prepares, or loads for transportation in commerce by rail one or more of the categories and quantities of rail security-sensitive materials set forth in §1580.100(b) of this part;

(3) Each rail hazardous materials receiver, located within a High Threat Urban Area (HTUA) that receives in commerce by rail or unloads one or more of the categories and quantities of rail security-sensitive materials set forth in §1580.100(b) of this part;

(4) Each passenger railroad carrier, including each carrier operating light rail or heavy rail transit service on track that is part of the general railroad system of transportation, each carrier operating or providing intercity passenger train service or commuter or other short-haul railroad passenger service in a metropolitan or suburban area (as described by 49 U.S.C. 20102), and each public authority operating passenger train service;

(5) Each passenger or freight railroad carrier hosting an operation described in paragraph (a)(4) of this section;

(6) Each tourist, scenic, historic, and excursion rail operator, whether operating on or off the general railroad system of transportation;

(7) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation; and

(8) Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.

(b) This part does not apply to a freight railroad carrier that operates rolling equipment only on track inside an installation that is not part of the general railroad system of transportation.

§ 1580.3 Terms used in this part.

For purposes of this part:

Commuter passenger train service means ''train, commuter'' as defined in 49 CFR 238.5, and includes a railroad operation that ordinarily uses diesel or electric powered locomotives and railroad passenger cars to serve an urban area, its suburbs, and more distant outlying communities in the greater metropolitan area. A commuter operation is part of the general railroad system of transportation regardless of whether it is physically connected to other railroads.

General railroad system of transportation means the network of standard gage track over which goods may be transported throughout the Nation and passengers may travel between cities and within metropolitan and suburban areas. *See* 49 CFR part 209, appendix A.

Hazardous material means ''hazardous material'' as defined in 49 CFR 171.8.

Heavy rail transit means service provided by self-propelled electric railcars, typically drawing power from a third rail, operating in separate rights-of-way in multiple cars; also referred to as subways, metros, or regional rail.

High Threat Urban Area (HTUA) means an area comprising one or more cities and surrounding areas including

a 10-mile buffer zone, as listed in appendix A to this part.

Improvised explosive device means a device fabricated in an improvised manner that incorporates explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in its design, and generally includes a power supply, a switch or timer, and a detonator or initiator.

Intercity passenger train service means both ''train, long-distance intercity passenger'' and ''train, short-distance intercity passenger'' as defined in 49 CFR 238.5.

Light rail transit means service provided by self-propelled electric railcars, typically drawing power from an overhead wire, operating in either exclusive or non-exclusive rights-of-way in single or multiple cars and with shorter distance trips and frequent stops; also referred to as streetcars, trolleys, and trams.

Offers or *offeror* means:

(1) Any person who does either or both of the following:

(i) Performs, or is responsible for performing, any pre-transportation function for transportation of the hazardous material in commerce.

(ii) Tenders or makes the hazardous material available to a carrier for transportation in commerce.

(2) A carrier is not an offeror when it performs a function required as a condition of acceptance of a hazardous material for transportation in commerce (such as reviewing shipping papers, examining packages to ensure that they are in conformance with the HMR, or preparing shipping documentation for its own use) or when it transfers a hazardous material to another carrier for continued transportation in commerce without performing a pre-transportation function. *See* 49 CFR 171.8.

Passenger car means rail rolling equipment intended to provide transportation for members of the general public and includes a self-propelled car designed to carry passengers, baggage, mail, or express. This term includes a passenger coach, cab car, and a Multiple Unit (MU) locomotive. In the context of articulated equipment, ''passenger car'' means that segment of the rail rolling equipment located between two trucks. This term does not include a private car. *See* 49 CFR 238.5.

Passenger train means a train that transports or is available to transport members of the general public. *See* 49 CFR 238.5.

Private car means rail rolling equipment that is used only for excursion, recreational, or private transportation purposes. A private car is not a passenger car. *See* 49 CFR 238.5.

Rail facility means a location at which rail cargo or infrastructure assets are stored, cargo is transferred between conveyances and/or modes of transportation, where transportation command and control operations are performed, or maintenance operations are performed. The term also includes, but is not limited to, passenger stations and terminals, rail yards, crew management centers, dispatching centers, transportation terminals and stations, fueling centers, and telecommunication centers.

Rail hazardous materials receiver means any operator of a fixed-site facility that has a physical connection to the general railroad system of transportation and receives or unloads from transportation in commerce by rail one or more of the categories and quantities of rail security-sensitive materials set forth in §1580.100(b) of this part, but does not include the operator of a facility owned or operated by a department, agency, or instrumentality of the Federal government.

Rail hazardous materials shipper means the operator of any fixed-site facility that has a physical connection to the general railroad system of transportation and offers, prepares, or loads for transportation by rail one or more of the categories and quantities of rail security-sensitive materials set forth in §1580.100(b) of this part, but does not include the operator of a facility owned or operated by a department, agency, or instrumentality of the Federal government.

Rail secure area means a secure location(s) identified by a rail hazardous materials shipper or rail hazardous materials receiver where security-related pre-transportation or transportation functions are performed or rail cars

containing the categories and quantities of rail security-sensitive materials are prepared, loaded, stored, and/or unloaded.

Rail security-sensitive material means one or more of the categories and quantities of hazardous materials set forth in § 1580.100(b) of this part.

Rail transit facility means rail transit stations, terminals, and locations at which rail transit infrastructure assets are stored, command and control operations are performed, or maintenance is performed. The term also includes rail yards, crew management centers, dispatching centers, transportation terminals and stations, fueling centers, and telecommunication centers.

Rail transit system or ''Rail Fixed Guideway System'' means any light, heavy, or rapid rail system, monorail, inclined plane, funicular, cable car, trolley, or automated guideway that traditionally does not operate on track that is part of the general railroad system of transportation.

Railroad means any form of nonhighway ground transportation that runs on rails or electromagnetic guideways, including: Commuter or other short-haul railroad passenger service in a metropolitan or suburban area and commuter railroad service that was operated by the Consolidated Rail Corporation on January 1, 1979; and high speed ground transportation systems that connect metropolitan areas, without regard to whether those systems use new technologies not associated with traditional railroads; but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation. The term includes rail transit service operating on track that is part of the general railroad system of transportation but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation. *See* 49 U.S.C. 20102(1).

Railroad carrier means a person providing railroad transportation. *See* 49 U.S.C. 20102(2).

Residue means the hazardous material remaining in a packaging, including a tank car, after its contents have been unloaded to the maximum extent practicable and before the packaging is either refilled or cleaned of hazardous material and purged to remove any hazardous vapors. *See* 49 CFR 171.8.

Tourist, scenic, historic, or excursion operation means a railroad operation that carries passengers, often using antiquated equipment, with the conveyance of the passengers to a particular destination not being the principal purpose. Train movements of new passenger equipment for demonstration purposes are not tourist, scenic, historic, or excursion operations. *See* 49 CFR 238.5.

Transit means mass transportation by a conveyance that provides regular and continuing general or special transportation to the public, but does not include school bus, charter, or sightseeing transportation. *See* 49 U.S.C 5302(a). Transit may occur on or off the general railroad system of transportation. For purposes of this part, the term ''transit'' excludes buses and commuter passenger train service.

Transportation or transport means the movement of property including loading, unloading, and storage. Transportation or transport also includes the movement of people, boarding, and disembarking incident to that movement.

§ 1580.5 Inspection authority.

(a) This section applies to the following:

(1) Each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.

(2) Each rail hazardous materials shipper.

(3) Each rail hazardous materials receiver located within an HTUA.

(4) Each passenger railroad carrier, including each carrier operating light rail or heavy rail transit service on track that is part of the general railroad system of transportation, each carrier operating or providing intercity passenger train service or commuter or other short-haul railroad passenger service in a metropolitan or suburban area (as described by 49 U.S.C. 20102), and each public authority operating passenger train service.

(5) Each passenger or freight railroad carrier hosting an operation described in paragraph (a)(4) of this section.

(6) Each tourist, scenic, historic, and excursion rail operator, whether operating on or off the general railroad system of transportation.

(7) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation.

(8) Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.

(b) The persons described in paragraph (a) of this section must allow TSA and other authorized DHS officials, at any time and in a reasonable manner, without advance notice, to enter, inspect, and test property, facilities, equipment, and operations; and to view, inspect, and copy records, as necessary to carry out TSA's security-related statutory or regulatory authorities, including its authority to—

(1) Assess threats to transportation;

(2) Enforce security-related regulations, directives, and requirements;

(3) Inspect, maintain, and test the security of facilities, equipment, and systems;

(4) Ensure the adequacy of security measures for the transportation of passengers and freight, including hazardous materials;

(5) Oversee the implementation, and ensure the adequacy, of security measures at rail yards, stations, terminals, transportation-related areas of rail hazardous materials shipper and receiver facilities, crew management centers, dispatch centers, telecommunication centers, and other transportation facilities and infrastructure;

(6) Review security plans; and

(7) Carry out such other duties, and exercise such other powers, relating to transportation security, as the Assistant Secretary of Homeland Security for the TSA considers appropriate, to the extent authorized by law.

(c) TSA and DHS officials working with TSA, may enter, without advance notice, and be present within any area or within any conveyance without access media or identification media issued or approved by a railroad carrier, rail transit system owner or operator, rail hazardous materials shipper, or rail hazardous materials receiver in order to inspect or test compliance, or perform other such duties as TSA may direct.

(d) TSA inspectors and DHS officials working with TSA will, on request, present their credentials for examination, but the credentials may not be photocopied or otherwise reproduced.

Subpart B—Freight Rail Including Freight Railroad Carriers, Rail Hazardous Materials Shippers, Rail Hazardous Materials Receivers, and Private Cars

§ 1580.100 Applicability.

(a) *Applicability.* The requirements of this subpart apply to:

(1) Each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.

(2) Each rail hazardous materials shipper.

(3) Each rail hazardous materials receiver located with an HTUA.

(4) Each freight railroad carrier hosting a passenger operation described in § 1580.1(a)(4) of this part.

(5) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation.

(b) *Rail security-sensitive materials.* The requirements of this subpart apply to:

(1) A rail car containing more than 2,268 kg (5,000 lbs) of a Division 1.1, 1.2, or 1.3 (explosive) material, as defined in 49 CFR 173.50;

(2) A tank car containing a material poisonous by inhalation as defined in 49 CFR 171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 CFR 173.115(c), and Division 6.1 liquids meeting the defining criteria in 49 CFR 173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 CFR 173.133(a), excluding residue quantities of these materials; and

(3) A rail car containing a highway route-controlled quantity of a Class 7

(radioactive) material, as defined in 49 CFR 173.403.

[73 FR 72173, Nov. 26, 2008, as amended at 74 FR 23656, May 20, 2009]

§ 1580.101 Rail security coordinator.

(a) *Applicability*. This section applies to:

(1) Each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.

(2) Each rail hazardous materials shipper.

(3) Each rail hazardous materials receiver located with an HTUA.

(4) Each freight railroad carrier hosting the passenger operations described in §1580.1(a)(4) of this part.

(5) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation, when notified by TSA in writing, that a threat exists concerning that operation.

(b) Each person described in paragraph (a) of this section must designate and use a primary and at least one alternate Rail Security Coordinator (RSC).

(c) The RSC and alternate(s) must be appointed at the corporate level.

(d) Each freight railroad carrier, rail hazardous materials shipper, and rail hazardous materials receiver required to have an RSC must provide to TSA the names, title, phone number(s), and e-mail address(es) of the RSCs and alternate RSCs, and must notify TSA within 7 calendar days when any of this information changes.

(e) Each freight railroad carrier, rail hazardous materials shipper, and rail hazardous materials receiver required to have an RSC must ensure that at least one RSC:

(1) Serves as the primary contact for intelligence information and security-related activities and communications with TSA. Any individual designated as an RSC may perform other duties in addition to those described in this section;

(2) Is available to TSA on a 24-hours a day, 7 days a week basis; and

(3) Coordinates security practices and procedures with appropriate law enforcement and emergency response agencies.

[73 FR 72173, Nov. 26, 2008, as amended at 74 FR 23656, May 20, 2009]

§ 1580.103 Location and shipping information for certain rail cars.

(a) *Applicability*. This section applies to:

(1) Each freight railroad carrier transporting one or more of the categories and quantities of rail security-sensitive materials.

(2) Each rail hazardous materials shipper.

(3) Each rail hazardous materials receiver located with an HTUA.

(b) *General requirement*. Each person described in paragraph (a) of this section must have procedures in place to determine the location and shipping information for each rail car under its physical custody and control that contains one or more of the categories and quantities of rail security-sensitive materials.

(c) *Required information*. The location and shipping information required in paragraph (b) of this section must include the following:

(1) The rail car's current location by city, county, and state, including, for freight railroad carriers, the railroad milepost, track designation, and the time that the rail car's location was determined.

(2) The rail car's routing, if a freight railroad carrier.

(3) A list of the total number of rail cars containing the materials listed in §1580.100(b) of this part, broken down by:

(i) The shipping name prescribed for the material in column 2 of the table in 49 CFR 172.101;

(ii) The hazard class or division number prescribed for the material in column 3 of the table in 49 CFR 172.101; and

(iii) The identification number prescribed for the material in column 4 of the table in 49 CFR 172.101.

(4) Each rail car's initial and number.

(5) Whether the rail car is in a train, rail yard, siding, rail spur, or rail hazardous materials shipper or receiver facility, including the name of the rail yard or siding designation.

(d) *Timing-class I freight railroad carriers.* Upon request by TSA, each Class I freight railroad carrier described in paragraph (a) of this section must provide the location and shipping information to TSA no later than:

(1) Five minutes if the request concerns only one rail car; and

(2) Thirty minutes if the request concerns two or more rail cars.

(e) *Timing-other than class I freight railroad carriers.* Upon request by TSA, all persons described in paragraph (a) of this section, other than Class I freight railroad carriers, must provide the location and shipping information to TSA no later than 30 minutes, regardless of the number of cars covered by the request.

(f) *Method.* All persons described in paragraph (a) of this section must provide the requested location and shipping information to TSA by one of the following methods:

(1) Electronic data transmission in spreadsheet format.

(2) Electronic data transmission in Hyper Text Markup Language (HTML) format.

(3) Electronic data transmission in Extensible Markup Language (XML).

(4) Facsimile transmission of a hard copy spreadsheet in tabular format.

(5) Posting the information to a secure website address approved by TSA.

(6) Another format approved by TSA.

(g) *Telephone number.* Each person described in paragraph (a) of this section must provide a telephone number for use by TSA to request the information required in paragraph (c) of this section.

(1) The telephone number must be monitored at all times.

(2) A telephone number that requires a call back (such as an answering service, answering machine, or beeper device) does not meet the requirements of this paragraph.

(h) *Definition.* As used in this section, *Class I* has the meaning assigned by regulations of the Surface Transportation Board (STB) (49 CFR part 1201; General Instructions 1–1).

[73 FR 72173, Nov. 26, 2008, as amended at 74 FR 23657, May 20, 2009]

§ 1580.105 Reporting significant security concerns.

(a) *Applicability.* This section applies to:

(1) Each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.

(2) Each rail hazardous materials shipper.

(3) Each rail hazardous materials receiver located with an HTUA.

(4) Each freight railroad carrier hosting a passenger operation described in § 1580.1(a)(4) of this part.

(5) Each operator of private cars, including business/office cars and circus, on or connected to the general railroad system of transportation.

(b) Each person described in paragraph (a) of this section must immediately report potential threats and significant security concerns to DHS by telephoning the Freedom Center at 1–866–615–5150.

(c) Potential threats or significant security concerns encompass incidents, suspicious activities, and threat information including, but not limited to, the following:

(1) Interference with the train crew.

(2) Bomb threats, specific and nonspecific.

(3) Reports or discovery of suspicious items that result in the disruption of railroad operations.

(4) Suspicious activity occurring onboard a train or inside the facility of a freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver that results in a disruption of operations.

(5) Suspicious activity observed at or around rail cars, facilities, or infrastructure used in the operation of the railroad, rail hazardous materials shipper, or rail hazardous materials receiver.

(6) Discharge, discovery, or seizure of a firearm or other deadly weapon on a train, in a station, terminal, facility, or storage yard, or other location used in the operation of the railroad, rail hazardous materials shipper, or rail hazardous materials receiver.

(7) Indications of tampering with rail cars.

(8) Information relating to the possible surveillance of a train or facility,

storage yard, or other location used in the operation of the railroad, rail hazardous materials shipper, or rail hazardous materials receiver.

(9) Correspondence received by the freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver indicating a potential threat. Other incidents involving breaches of the security of the freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver's operations or facilities.

(d) Information reported should include, as available and applicable:

(1) The name of the reporting freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver and contact information, including a telephone number or e-mail address.

(2) The affected train, station, terminal, rail hazardous materials facility, or other rail facility or infrastructure.

(3) Identifying information on the affected train, train line, and route.

(4) Origination and termination locations for the affected train, including departure and destination city and the rail line and route, as applicable.

(5) Current location of the affected train.

(6) Description of the threat, incident, or activity.

(7) The names and other available biographical data of individuals involved in the threat, incident, or activity.

(8) The source of any threat information.

[73 FR 72173, Nov. 26, 2008, as amended at 74 FR 23657, May 20, 2009]

§ 1580.107 Chain of custody and control requirements.

(a) *Within or outside of an HTUA, rail hazardous materials shipper transferring to carrier.* Except as provided in paragraph (g) of this section, at each location within or outside of an HTUA, a rail hazardous materials shipper transferring custody of a rail car containing one or more of the categories and quantities of rail security-sensitive materials to a freight railroad carrier must:

(1) Physically inspect the rail car before loading for signs of tampering, including closures and seals; other signs that the security of the car may have been compromised; suspicious items or items that do not belong, including the presence of an improvised explosive device.

(2) Keep the rail car in a rail secure area from the time the security inspection required by paragraph (a)(1) of this section or by 49 CFR 173.31(d), whichever occurs first, until the freight railroad carrier takes physical custody of the rail car.

(3) Document the transfer of custody to the railroad carrier in writing or electronically.

(b) *Within or outside of an HTUA, carrier receiving from a rail hazardous materials shipper.* At each location within or outside of an HTUA where a freight railroad carrier receives from a rail hazardous materials shipper custody of a rail car containing one or more of the categories and quantities of rail security-sensitive materials, the freight railroad carrier must document the transfer in writing or electronically and perform the required security inspection in accordance with 49 CFR 174.9.

(c) *Within an HTUA, carrier transferring to carrier.* Within an HTUA, whenever a freight railroad carrier transfers a rail car containing one or more of the categories and quantities of rail security-sensitive materials to another freight railroad carrier, each freight railroad carrier must adopt and carry out procedures to ensure that the rail car is not left unattended at any time during the physical transfer of custody. These procedures must include the receiving freight railroad carrier performing the required security inspection in accordance with 49 CFR 174.9. Both the transferring and the receiving railroad carrier must document the transfer of custody in writing or electronically.

(d) *Outside of an HTUA, carrier transferring to carrier.* Outside an HTUA, whenever a freight railroad carrier transfers a rail car containing one or more of the categories and quantities of rail security-sensitive materials to another freight railroad carrier, and the rail car containing this hazardous material may subsequently enter an HTUA, each freight railroad carrier must adopt and carry out procedures to

ensure that the rail car is not left unattended at any time during the physical transfer of custody. These procedures must include the receiving railroad carrier performing the required security inspection in accordance with 49 CFR 174.9. Both the transferring and the receiving railroad carrier must document the transfer of custody in writing or electronically.

(e) *Within an HTUA, carrier transferring to rail hazardous materials receiver.* A freight railroad carrier delivering a rail car containing one or more of the categories and quantities of rail security-sensitive materials to a rail hazardous materials receiver located within an HTUA must not leave the rail car unattended in a non-secure area until the rail hazardous materials receiver accepts custody of the rail car. Both the railroad carrier and the rail hazardous materials receiver must document the transfer of custody in writing or electronically.

(f) *Within an HTUA, rail hazardous materials receiver receiving from carrier.* Except as provided in paragraph (j) of this section, a rail hazardous materials receiver located within an HTUA that receives a rail car containing one or more of the categories and quantities of rail security-sensitive materials from a freight railroad carrier must:

(1) Ensure that the rail hazardous materials receiver or railroad carrier maintains positive control of the rail car during the physical transfer of custody of the rail car.

(2) Keep the rail car in a rail secure area until the car is unloaded.

(3) Document the transfer of custody from the railroad carrier in writing or electronically.

(g) *Within or outside of an HTUA, rail hazardous materials receiver rejecting car.* This section does not apply to a rail hazardous materials receiver that does not routinely offer, prepare, or load for transportation by rail one or more of the categories and quantities of rail security-sensitive materials. If such a receiver rejects and returns a rail car containing one or more of the categories and quantities of rail security-sensitive materials to the originating offeror or shipper, the requirements of this section do not apply to the receiver. The requirements of this section do apply to any railroad carrier to which the receiver transfers custody of the rail car.

(h) *Document retention.* Covered entities must maintain the documents required under this section for at least 60 calendar days and make them available to TSA upon request.

(i) *Rail secure area.* The rail hazardous materials shipper and the rail hazardous materials receiver must use physical security measures to ensure that no unauthorized person gains access to the rail secure area.

(j) *Exemption for rail hazardous materials receivers.* A rail hazardous materials receiver located within an HTUA may request from TSA an exemption from some or all of the requirements of this section if the receiver demonstrates that the potential risk from its activities is insufficient to warrant compliance with this section. TSA will consider all relevant circumstances, including—

(1) The amounts and types of all hazardous materials received.

(2) The geography of the area surrounding the receiver's facility.

(3) Proximity to entities that may be attractive targets, including other businesses, housing, schools, and hospitals.

(4) Any information regarding threats to the facility.

(5) Other circumstances that indicate the potential risk of the receiver's facility does not warrant compliance with this section.

(k) *Terms used in this section.* (1) As used in this section, a rail car is *attended* if an employee or authorized representative:

(i) Is physically located on site in reasonable proximity to the rail car;

(ii) Is capable of promptly responding to unauthorized access or activity at or near the rail car, including immediately contacting law enforcement or other authorities; and

(iii) Immediately responds to any unauthorized access or activity at or near the rail car either personally or by contacting law enforcement or other authorities.

(2) As used in this section, *maintains positive control* means that the rail hazardous materials receiver and the railroad carrier communicate and cooperate with each other to provide for the security of the rail car during the physical transfer of custody. *Attending* the rail car is a component part of maintaining positive control.

(3) As used in this section, *document the transfer* means documentation uniquely identifying that the rail car was attended during the transfer of custody, including:

(i) Car initial and number.

(ii) Identification of individuals who attended the transfer (names or uniquely identifying employee number).

(iii) Location of transfer.

(iv) Date and time the transfer was completed.

[73 FR 72173, Nov. 26, 2008, as amended at 74 FR 23657, May 20, 2009]

§ 1580.109 Preemptive effect.

Under 49 U.S.C. 20106, issuance of the regulations in this part preempts any State law, regulation, or order covering the same subject matter, except an additional or more stringent law, regulation, or order that is necessary to eliminate or reduce an essentially local security hazard; that is not incompatible with a law, regulation, or order of the United States Government; and that does not unreasonably burden interstate commerce. For example, under 49 U.S.C. 20106, issuance of §1580.107 of this subpart preempts any State or tribal law, rule, regulation, order or common law requirement covering the same subject matter.

§ 1580.111 Harmonization of federal regulation of nuclear facilities.

TSA will coordinate activities under this subpart with the Nuclear Regulatory Commission (NRC) and the Department of Energy (DOE) with respect to regulation of rail hazardous materials shippers and receivers that are also licensed or regulated by the NRC or DOE under the Atomic Energy Act of 1954, as amended, to maintain consistency with the requirements imposed by the NRC and DOE.

Subpart C—Passenger Rail Including Passenger Railroad Carriers, Rail Transit Systems, Tourist, Scenic, Historic and Excursion Operators, and Private Cars

§ 1580.200 Applicability.

This subpart includes requirements for:

(a) Each passenger railroad carrier, including each carrier operating light rail or heavy rail transit service on track that is part of the general railroad system of transportation, each carrier operating or providing intercity passenger train service or commuter or other short-haul railroad passenger service in a metropolitan or suburban area (as described by 49 U.S.C. 20102), and each public authority operating passenger train service.

(b) Each passenger railroad carrier hosting an operation described in paragraph (a) of this section.

(c) Each tourist, scenic, historic, and excursion rail operator, whether operating on or off the general railroad system of transportation.

(d) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation.

(e) Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.

§ 1580.201 Rail security coordinator.

(a) *Applicability*. This section applies to:

(1) Each passenger railroad carrier, including each carrier operating light rail or heavy rail transit service on track that is part of the general railroad system of transportation, each carrier operating or providing intercity passenger train service or commuter or other short-haul railroad passenger service in a metropolitan or suburban area (as described by 49 U.S.C. 20102), and each public authority operating passenger train service.

(2) Each passenger railroad carrier hosting an operation described in paragraph (a)(1) of this section.

(3) Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.

(4) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation, when notified by TSA, in writing, that a security threat exists concerning that operation.

(5) Each tourist, scenic, historic, or excursion operations, whether on or off the general railroad system of transportation, when notified by TSA, in writing, that a security threat exists concerning that operation.

(b) Each person described in paragraph (a) of this section must designate and use a primary and at least one alternate RSC.

(c) The RSC and alternate(s) must be appointed at the corporate level.

(d) Each passenger railroad carrier and rail transit system required to have an RSC must provide to TSA the names, titles, phone number(s), and e-mail address(es) of the RSCs, and alternate RSCs, and must notify TSA within 7 calendar days when any of this information changes.

(e) Each passenger railroad carrier and rail transit system required to have an RSC must ensure that at least one RSC:

(1) Serves as the primary contact for intelligence information and security-related activities and communications with TSA. Any individual designated as an RSC may perform other duties in addition to those described in this section.

(2) Is available to TSA on a 24-hours a day, 7 days a week basis.

(3) Coordinate security practices and procedures with appropriate law enforcement and emergency response agencies.

§ 1580.203 Reporting significant security concerns.

(a) *Applicability*. This section applies to:

(1) Each passenger railroad carrier, including each carrier operating light rail or heavy rail transit service on track that is part of the general railroad system of transportation, each carrier operating or providing intercity passenger train service or commuter or other short-haul railroad passenger service in a metropolitan or suburban area (as described by 49 U.S.C. 20102), and each public authority operating passenger train service.

(2) Each passenger railroad carrier hosting an operation described in paragraph (a)(1) of this section.

(3) Each tourist, scenic, historic, and excursion rail operator, whether operating on or off the general railroad system of transportation.

(4) Each operator of private cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation.

(5) Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.

(b) Each person described in paragraph (a) of this section must immediately report potential threats and significant security concerns to DHS by telephoning the Freedom Center at 1–866–615–5150.

(c) Potential threats or significant security concerns encompass incidents, suspicious activities, and threat information including, but not limited to, the following:

(1) Interference with the train or transit vehicle crew.

(2) Bomb threats, specific and non-specific.

(3) Reports or discovery of suspicious items that result in the disruption of rail operations.

(4) Suspicious activity occurring onboard a train or transit vehicle or inside the facility of a passenger railroad carrier or rail transit system that results in a disruption of rail operations.

(5) Suspicious activity observed at or around rail cars or transit vehicles, facilities, or infrastructure used in the operation of the passenger railroad carrier or rail transit system.

(6) Discharge, discovery, or seizure of a firearm or other deadly weapon on a train or transit vehicle or in a station, terminal, facility, or storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system.

(7) Indications of tampering with passenger rail cars or rail transit vehicles.

(8) Information relating to the possible surveillance of a passenger train or rail transit vehicle or facility, storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system.

(9) Correspondence received by the passenger railroad carrier or rail transit system indicating a potential threat to rail transportation.

(10) Other incidents involving breaches of the security of the passenger railroad carrier or the rail transit system operations or facilities.

(d) Information reported should include, as available and applicable:

(1) The name of the passenger railroad carrier or rail transit system and contact information, including a telephone number or e-mail address.

(2) The affected station, terminal, or other facility.

(3) Identifying information on the affected passenger train or rail transit vehicle including number, train or transit line, and route, as applicable.

(4) Origination and termination locations for the affected passenger train or rail transit vehicle, including departure and destination city and the rail or transit line and route.

(5) Current location of the affected passenger train or rail transit vehicle.

(6) Description of the threat, incident, or activity.

(7) The names and other available biographical data of individuals involved in the threat, incident, or activity.

(8) The source of any threat information.

[73 FR 72173, Nov. 26, 2008, as amended at 74 FR 23657, May 20, 2009]

APPENDIX A TO PART 1580—HIGH THREAT URBAN AREAS (HTUAS)

State	Candidate urban area	Geographic area captured in the data count	Previously designated urban areas included
AZ	Phoenix Area *	Chandler, Gilbert, Glendale, Mesa, Peoria, Phoenix, Scottsdale, Tempe, and a 10-mile buffer extending from the border of the combined area.	Phoenix, AZ.
CA	Anaheim/Santa Ana Area.	Anaheim, Costa Mesa, Garden Grove, Fullerton, Huntington Beach, Irvine, Orange, Santa Ana, and a 10-mile buffer extending from the border of the combined area.	Anaheim, CA; Santa Ana, CA.
	Bay Area	Berkeley, Daly City, Fremont, Hayward, Oakland, Palo Alto, Richmond, San Francisco, San Jose, Santa Clara, Sunnyvale, Vallejo, and a 10-mile buffer extending from the border of the combined area.	San Francisco, CA; San Jose, CA; Oakland, CA.
	Los Angeles/Long Beach Area.	Burbank, Glendale, Inglewood, Long Beach, Los Angeles, Pasadena, Santa Monica, Santa Clarita, Torrance, Simi Valley, Thousand Oaks, and a 10-mile buffer extending from the border of the combined area.	Los Angeles, CA; Long Beach, CA.
	Sacramento Area *	Elk Grove, Sacramento, and a 10-mile buffer extending from the border of the combined area.	Sacramento, CA.
	San Diego Area *	Chula Vista, Escondido, and San Diego, and a 10-mile buffer extending from the border of the combined area.	San Diego, CA.
CO	Denver Area	Arvada, Aurora, Denver, Lakewood, Westminster, Thornton, and a 10-mile buffer extending from the border of the combined area.	Denver, CO.
DC	National Capital Region.	National Capital Region and a 10-mile buffer extending from the border of the combined area.	National Capital Region, DC.
FL	Fort Lauderdale Area.	Fort Lauderdale, Hollywood, Miami Gardens, Miramar, Pembroke Pines, and a 10-mile buffer extending from the border of the combined area.	N/A.
	Jacksonville Area	Jacksonville and a 10-mile buffer extending from the city border	Jacksonville, FL.
	Miami Area	Hialeah, Miami, and a 10-mile buffer extending from the border of the combined area.	Miami, FL.
	Orlando Area	Orlando and a 10-mile buffer extending from the city border	Orlando, FL.
	Tampa Area *	Clearwater, St. Petersburg, Tampa, and a 10-mile buffer extending from the border of the combined area.	Tampa, FL.
GA	Atlanta Area	Atlanta and a 10-mile buffer extending from the city border	Atlanta, GA.
HI	Honolulu Area	Honolulu and a 10-mile buffer extending from the city border	Honolulu, HI.
IL	Chicago Area	Chicago and a 10-mile buffer extending from the city border	Chicago, IL.
IN	Indianapolis Area	Indianapolis and a 10-mile buffer extending from the city border	Indianapolis, IN.
KY	Louisville Area *	Louisville and a 10-mile buffer extending from the city border	Louisville, KY.

State	Candidate urban area	Geographic area captured in the data count	Previously designated urban areas included
LA	Baton Rouge Area*.	Baton Rouge and a 10-mile buffer extending from the city border	Baton Rouge, LA.
	New Orleans Area	New Orleans and a 10-mile buffer extending from the city border	New Orleans, LA.
MA	Boston Area	Boston, Cambridge, and a 10-mile buffer extending from the border of the combined area.	Boston, MA.
MD	Baltimore Area	Baltimore and a 10-mile buffer extending from the city border	Baltimore, MD.
MI	Detroit Area	Detroit, Sterling Heights, Warren, and a 10-mile buffer extending from the border of the combined area.	Detroit, MI.
MN	Twin Cities Area	Minneapolis, St. Paul, and a 10-mile buffer extending from the border of the combined entity.	Minneapolis, MN; St. Paul, MN.
MO	Kansas City Area	Independence, Kansas City (MO), Kansas City (KS), Olathe, Overland Park, and a 10-mile buffer extending from the border of the combined area.	Kansas City, MO.
	St. Louis Area	St. Louis and a 10-mile buffer extending from the city border	St. Louis, MO.
NC	Charlotte Area	Charlotte and a 10-mile buffer extending from the city border	Charlotte, NC.
NE	Omaha Area*	Omaha and a 10-mile buffer extending from the city border	Omaha, NE.
NJ	Jersey City/Newark Area.	Elizabeth, Jersey City, Newark, and a 10-mile buffer extending from the border of the combined area.	Jersey City, NJ; Newark, NJ.
NV	Las Vegas Area*	Las Vegas, North Las Vegas, and a 10-mile buffer extending from the border of the combined entity.	Las Vegas, NV.
NY	Buffalo Area*	Buffalo and a 10-mile buffer extending from the city border	Buffalo, NY.
	New York City Area.	New York City, Yonkers, and a 10-mile buffer extending from the border of the combined area.	New York, NY.
OH	Cincinnati Area	Cincinnati and a 10-mile buffer extending from the city border	Cincinnati, OH.
	Cleveland Area	Cleveland and a 10-mile buffer extending from the city border	Cleveland, OH.
	Columbus Area	Columbus and a 10-mile buffer extending from the city border	Columbus, OH.
	Toledo Area*	Oregon, Toledo, and a 10-mile buffer extending from the border of the combined area.	Toledo, OH.
OK	Oklahoma City Area*.	Norman, Oklahoma and a 10-mile buffer extending from the border of the combined area.	Oklahoma City, OK.
OR	Portland Area	Portland, Vancouver, and a 10-mile buffer extending from the border of the combined area.	Portland, OR.
PA	Philadelphia Area	Philadelphia and a 10-mile buffer extending from the city border	Philadelphia, PA.
	Pittsburgh Area	Pittsburgh and a 10-mile buffer extending from the city border	Pittsburgh, PA.
TN	Memphis Area	Memphis and a 10-mile buffer extending from the city border	Memphis, TN.
TX	Dallas/Fort Worth/Arlington Area.	Arlington, Carrollton, Dallas, Fort Worth, Garland, Grand Prairie, Irving, Mesquite, Plano, and a 10-mile buffer extending from the border of the combined area.	Dallas, TX; Fort Worth, TX; Arlington, TX.
	Houston Area	Houston, Pasadena, and a 10-mile buffer extending from the border of the combined entity.	Houston, TX.
	San Antonio Area	San Antonio and a 10-mile buffer extending from the city border	San Antonio, TX.
WA	Seattle Area	Seattle, Bellevue, and a 10-mile buffer extending from the border of the combined area.	Seattle, WA.
WI	Milwaukee Area	Milwaukee and a 10-mile buffer extending from the city border	Milwaukee, WI.

*FY05 Urban Areas eligible for sustainment funding through the FY06 Urban Areas Security Initiative (UASI) program; any Urban Area not identified as eligible through the risk analysis process for two consecutive years will not be eligible for continued funding under the UASI program.

APPENDIX B TO PART 1580—SUMMARY OF THE APPLICABILITY OF PART 1580

[This is a summary—see body of text for complete requirements]

Security measure and rule section	Freight railroad carriers NOT transporting specified hazardous materials	Freight railroad carriers transporting specified hazardous materials (§ 1580.100(b))	Rail operations at certain facilities that ship (*i.e.*, offer, prepare, or load for transportation) hazardous materials	Rail operations at certain facilities that receive or unload hazardous materials within an HTUA	Passenger railroad carriers and rail transit systems	Certain other rail operations (private, business/office, circus, tourist, historic, excursion)
Allow TSA to inspect (§ 1580.5)	X	X	X	X	X	X
Appoint rail security coordinator (§ 1580.101 freight; § 1580.201 passenger)	X	X	X	X	X	[1]
Report significant security concerns (§ 1580.105 freight; § 1580.203 passenger)	X	X	X	X	X	X
Provide location and shipping information for rail cars containing specified hazardous materials if requested (§ 1580.103)		X	X	X		
Chain of custody and control requirements for transport of specified hazardous materials that are or may be in HTUA (§ 1580.107)		X	X	X		

[1] Only if notified in writing that a security threat exists.