[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Parts 1515, 1520, 1522, 1540, 1544, 1546, 1548, and 1549

[Docket No. TSA-2009-0018; Amendment Nos. 1515-1, 1520-8, 1522-New, 1540-10, 1544-9, 1546-5, 1548-5, 1549-New]

RIN 1652-AA64

Air Cargo Screening

AGENCY: Transportation Security Administration, DHS.

ACTION: Interim final rule; request for comments.

SUMMARY: This rule codifies a statutory requirement of the Implementing Recommendations of the 9/11 Commission Act that the Transportation Security Administration (TSA) establish a system to screen 100 percent of cargo transported on passenger aircraft by August 3, 2010. To assist in carrying out this mandate, this rule establishes a program under which TSA will certify cargo screening facilities located in the U.S. that volunteer to screen cargo prior to tendering it to aircraft operators for carriage on passenger aircraft. This rule requires affected passenger aircraft operators to ensure that either an aircraft operator or certified cargo screening facility that does so in accordance with TSA standards, or TSA itself, screens all cargo loaded on passenger aircraft.

TSA will require certified cargo screening facilities (CCSFs) to screen cargo using TSA-approved methods and implement chain of custody measures to ensure the security of the screened cargo throughout the air cargo supply chain prior to tendering it

for transport on passenger aircraft. CCSF personnel must successfully undergo a TSA-conducted security threat assessment (STA) and pay a fee for that assessment. TSA proposes a fee to cover the Government's costs in conducting the STA and requests comment on the fee and the methodology used to develop the fee.

Before being certified and periodically thereafter, the CCSF must undergo examination by a TSA-approved validator. Validators must have specified qualifications, complete training regarding the certified cargo screening program (CCSP), and successfully undergo a TSA-conducted STA as described in the discussion of part 1540 in this preamble, and pay a fee for that assessment.

DATES: Effective Date: This rule is effective [Insert date 60 days after date of publication in the Federal Register].

Comment Date: Comments must be received by [Insert date 60 days after date of publication in the Federal Register].

ADDRESSES: You may submit comments, identified by the TSA docket number to this rulemaking, to the Federal Docket Management System (FDMS), a government-wide, electronic docket management system, using any one of the following methods:

Electronically: You may submit comments through the Federal eRulemaking portal at http://www.regulations.gov. Follow the online instructions for submitting comments.

Mail, In Person, or Fax: Address, hand-deliver, or fax your written comments to the Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building Ground Floor, Room W12-140, Washington, DC 20590-0001; Fax 202-493-2251. The Department of Transportation (DOT), which maintains

and processes TSA's official regulatory dockets, will scan the submission and post it to FDMS.

See SUPPLEMENTARY INFORMATION for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: Tamika McCree, Manager, Air Cargo Stakeholder Relations, Air Cargo Security, TSA-28, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598-6028; telephone (571) 227-2632; facsimile (571) 227-1947; e-mail AirCargoScreeningCommentsIFR@dhs.gov.

SUPPLEMENTARY INFORMATION:

Comments Invited

TSA adopts this interim rule without prior notice and prior public comment. In this rule, however, TSA seeks prior public comment on our proposed fee to cover the cost of the STAs. To the maximum extent possible, DHS provides an opportunity for public comment on regulations issued without prior notice. Accordingly, TSA invites interested persons to participate in this rulemaking by submitting written comments, data, or views on the proposed fee for the STA, as well as all other aspects of this rule. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking action. See ADDRESSES above for information on where to submit comments.

With each comment, please identify the docket number at the beginning of your comments. TSA encourages commenters to provide their names and addresses. The most helpful comments reference a specific portion of the rulemaking, explain the reason for any recommended change, and include supporting data. You may submit comments

and material electronically, in person, by mail, or fax as provided under ADDRESSES**,** but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you would like TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it to you.

TSA will file in the public docket all comments received by TSA, except for comments containing confidential information and sensitive security information (SSI)[1], TSA will consider all comments received on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Confidential or Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in FOR FURTHER INFORMATION CONTACT section.

[1] "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold documents containing SSI, confidential business information, or trade secrets in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA determines, however, that portions of these comments may be made publicly available, TSA may include a redacted version of the comment in the public docket. If TSA receives a request to examine or copy information that is not in the public docket, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the FOIA regulation of the Department of Homeland Security found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual who submitted the comment (or signed the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published in the Federal Register on April 11, 2000 (65 FR 19477) and modified on January 17, 2008 (73 FR 3316).

You may review TSA's electronic public docket on the Internet at http://www.regulations.gov. In addition, DOT's Docket Management Facility provides a physical facility, staff, equipment, and assistance to the public. To obtain assistance or to review comments in TSA's public docket, you may visit this facility between 9:00 a.m. to 5:00 p.m., Monday through Friday, excluding legal holidays, or call (202) 366-9826.

This docket operations facility is located in the West Building Ground Floor, Room W12-140 at 1200 New Jersey Avenue, SE, Washington, DC 20590.

Availability of Rulemaking Document

You can get an electronic copy using the Internet by--

(1) Searching the electronic Federal Docket Management System (FDMS) web page at http://www.regulations.gov;

(2) Accessing the Government Printing Office's web page at http://www.gpoaccess.gov/fr/index.html; or

(3) Visiting TSA's Security Regulations web page at http://www.tsa.gov and accessing the link for "Research Center" at the top of the page.

In addition, copies are available by writing or calling the individual in the FOR FURTHER INFORMATION CONTACT section. Make sure to identify the docket number of this rulemaking.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires TSA to comply with small entity requests for information and advice about compliance with statutes and regulations within TSA's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in FOR FURTHER INFORMATION CONTACT. Persons can obtain further information regarding SBREFA on the Small Business Administration's web page at http://www.sba.gov/advo/laws/law_lib.html.

Abbreviations and Terms Used in This Document

CBP	U.S. Customs and Border Protection
CCSF	Certified Cargo Screening Facility

CCSP	Certified Cargo Screening Program
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
DHS	Department of Homeland Security
FSD	Federal Security Director
IAC	Indirect Air Carrier
IED	Improvised Explosive Device
MSP	Model Security Program
SIDA	Security Identification Display Area
SSI	Sensitive Security Information
STA	Security Threat Assessment
TSA	Transportation Security Administration

Outline of Interim Final Rule

I. Summary of Rule

II. Background

A. Current Air Cargo Screening

B. 9/11 Act Requirements

C. Development of the Certified Cargo Screening Program

D. Certified Cargo Screening Pilot Programs

III. TSA's Program for Achieving the Statutory Mandates for Cargo Loaded Domestically

IV. Organization of the Rule

V. Section-by-Section Analysis

I. Summary of Rule

This rule provides that affected U.S. aircraft operators and foreign air carriers[2] must have screened at least 50 percent of its cargo transported on passenger aircraft by February 3, 2009, and must screen 100 percent of cargo by August 3, 2010, to carry out sec. 1602 of the Implementing the Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53, 121 Stat. 266, 478, Aug. 3, 2007) (9/11 Act). The rule applies to certain commercial passenger operations, and applies to foreign air carriers the same standards that apply to U.S. aircraft

[2] The affected aircraft operators are U.S. aircraft operators with full programs under 49 CFR 1544.101(a) and foreign air carriers with security programs under 49 CFR 1546.101(a) or (b). This includes aircraft operators with scheduled or public charter operations with an aircraft having a passenger seating configuration of 61 or more seats, and those operating smaller aircraft when passengers are enplaned from or deplaned into a sterile area.

operators, for the same types of flights. This rule applies only to cargo loaded in the United States. It does not apply to either U.S. aircraft operators or foreign air carriers when they load cargo outside the U.S. and transport it into the U.S., nor to U.S. or foreign all-cargo operations. This rule will not cover general aviation operations.

The Transportation Security Administration (TSA) concluded that this mandate could not be achieved by relying solely on U.S. aircraft operators and foreign air carriers to conduct screening. Aircraft operators do not have the capacity to screen the approximately 12 million pounds of cargo that is now transported on passenger aircraft daily. Requiring passenger aircraft operators to screen 100 percent of air cargo would result in carrier delays, backlogs of unscreened cargo, and missed flights, which could significantly impede the flow of commerce.

Accordingly, TSA will establish the certified cargo screening program (CCSP) to allow entities other than aircraft operators to conduct screening off-airport. Under the CCSP, facilities upstream in the air cargo supply chain, such as shippers, manufacturers, warehousing entities, distributors, third party logistics companies, and Indirect Air Carriers (IACs) that are located in the U.S., may apply to TSA to become certified cargo screening facilities (CCSFs). Aircraft operators that screen cargo off-airport must also become CCSFs in order to screen cargo for transport on passenger aircraft. These applicants must submit to TSA an application for certification of a single facility, including a TSA-approved validator's evaluation of the applicant's security measures. Once certified, the CCSF must--

- Implement the certified cargo screening standard security program that TSA develops and any amendments to it;
- Appoint security coordinators at the corporate and facility levels and alternates to be available 24 hours per day, 7 days per week;
- Ensure that the following individuals successfully undergo a TSA-conducted STA: (1) each employee and authorized representative who screens cargo or has unescorted access to screened cargo, and (2) each security coordinator and alternate, senior manager of the facility, and other individual who implements the cargo screening program;
- Adhere to strict physical and access control measures for the storage, handling, and screening of cargo;
- Screen cargo using TSA-approved methods;
- Implement chain of custody requirements, including the use of tamper evident technology, which must begin when the cargo is screened and remain intact until the cargo is tendered to the aircraft operator for transport on a passenger aircraft; and
- Apply for recertification, including a new examination by a TSA-approved validator, every 36 months.

TSA believes that it is important for CCSFs to submit to a recertification assessment of their security programs every three years in order to maintain good standing in the CCSP. Within the 36 month period, TSA will inspect the CCSF for compliance and the CCSFs will conduct quarterly self-audits. TSA based the 36-month

cycle on a similar program in the United Kingdom, the Known Consignor program discussed in section II.C. below.

This rule establishes procedures under which firms may apply for TSA's approval to conduct validation assessments of CCSF facilities. Approved validation firms must hold and carry out a TSA-approved security program, must have security coordinators to be the primary point of contact for security at the facility, and must ensure that individuals conducting assessments have professional qualifications, receive training, do not have conflicts of interest with facilities to be assessed, and conduct assessments impartially. The rule requires validators and their supervisors and validation firm security coordinators and their alternates to successfully undergo a TSA-conducted STA. Individuals conducting validation assessments must--

- Be a citizen or national of the United States or be a lawful permanent resident alien;
- Hold a certification or accreditation from a TSA-recognized organization qualified to certify or accredit a validator;
- Have at least five years of experience in inspection or validating compliance with certain government and industry organizations;
- Have sufficient knowledge of certain regulations, policies, and security programs and be able to determine compliance;
- Have sufficient knowledge of the CCSP; and
- Conduct no more than two assessments of a facility seeking approval, unless TSA authorizes otherwise.

This rule also amends the threat assessment provisions that currently exist in 49 CFR part 1540, subpart C, for individuals who work in the air cargo sector to enhance TSA's ability to effectively conduct STAs.

II. Background

A. Current Air Cargo Screening

Since 2002, TSA has implemented a multilayered, risk-based system for securing cargo transported on passenger aircraft. U.S. aircraft operators and foreign air carriers must ensure that cargo transported on passenger aircraft is screened or inspected as set forth in their security programs. 49 CFR 1544.205, 1546.205. IACs must screen a certain percentage of cargo prior to tendering the cargo for transport or take other security measures as required in the applicable Security Directives and in their security programs.[3] U.S. aircraft operators, foreign air carriers, and IACs must screen 100 percent of cargo considered to present an "elevated risk," and TSA screens 100 percent of all cargo transported on passenger aircraft at Category II-IV airports.[4]

Currently, aircraft operators conduct screening of most cargo at the airports. Generally applicable TSA-approved methods of screening include x-ray, explosives trace detection (ETD), explosive detection systems (EDS), explosives detection canine teams, and physical inspection along with verification of the description of the cargo on the shipping manifest. There are certain categories of cargo for which these generally

[3] Security Directives and security programs are SSI and the details are non-public information. See footnote 1.

[4] There are several categories of airport designations that are based largely on the number of enplanements. Category II-IV airports include those with less than five million annual domestic enplanements or with five million or more annual domestic enplanements, but less than one million international enplanements. Overall, approximately 99 percent of cargo loaded on passenger aircraft in the United States is loaded at Category X and I airports.

applicable methods of screening may not be effective or feasible, so the aircraft operators and IACs use TSA-approved alternative methods of screening.

B. 9/11 Act Requirements

The 9/11 Act amended 49 U.S.C. 44901(g)(1), which provides, in pertinent part:

> Not later than 3 years after the date of enactment of the [9/11 Act], the Secretary of Homeland Security shall establish a system to screen 100 percent of cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure the security of all such passenger aircraft carrying cargo.

As amended by the 9/11 Act, 49 U.S.C. 44901(g)(2) provides that the system used to screen cargo on passenger aircraft shall provide a level of security "commensurate with the level of security for the screening of passenger checked baggage" and directs that--

- Fifty percent of such cargo must be screened not later than February 3, 2009; and
- One hundred percent of such cargo must be screened not later than August 3, 2010.

Section 44901(g)(3)(B) explicitly authorizes TSA to issue an interim final rule (IFR) to implement the requirements. If TSA issues an IFR, TSA must issue a final rule not later than one year after the effective date of the IFR.

The 9/11 Act defines the term "screening" in sec. 44901(g)(5) to mean "a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security. Methods include x-ray systems, explosives detection systems, explosives trace detection, explosives detection canine teams certified by TSA or a physical search together with manifest verification." This section further provides that TSA may approve additional methods to ensure that the cargo does not pose a threat to transportation security and to assist in meeting the requirements of the 9/11 Act. TSA

will continue to consider different technologies or methods for screening cargo transported on passenger or cargo flights. TSA would approve these additional methods and technologies based on their applicability and effectiveness in screening specific commodities.

C. Development of the Certified Cargo Screening Program

TSA recognized that it needed to develop a program that could achieve the 9/11 Act's requirement for 100 percent screening while still allowing for the flow of commerce. Approximately 12 million pounds of cargo are transported on passenger aircraft in the United States each day. In evaluating the practical implications of 100 percent screening, the Congressional Research Service has stated that ". . . given the sheer volume of cargo that must be expediently processed and loaded on aircraft . . . full screening of air cargo, as is now required of checked passenger baggage, is likely to present significant logistic and operational challenges." CRS Report for Congress, Air Cargo Security, Updated July 30, 2007, CRS-2.

TSA has developed the CCSP by working closely with U.S. and international agencies and associations to incorporate key aspects of similar security programs in other countries and in the United States. In particular, TSA studied the Known Consignor programs in Great Britain and Ireland. Such programs have been in effect for several years and operate successfully. TSA also examined the security measures of the Customs-Trade Partnership Against Terrorism (C-TPAT), a U.S. Customs and Border Protection (CBP) program. Like the programs in Great Britain and Ireland, CBP's C-TPAT program adopts the concept of supply chain security in its voluntary program under which participants benefit from expedited CBP processing.

The United Kingdom (UK) Known Consignor program has key features that TSA has incorporated into the CCSP. First, like the CCSP, the UK Known Consignor program relies on authorized entities to augment air carriers' screening of cargo. Both programs rely on a chain of custody concept, requiring verification that no tampering has occurred between the time of screening and the time the cargo is tendered to the air carrier.

Second, the UK Known Consignor program requires approved validators to assess Known Consignors and requires Known Consignors to pay a fee for these assessments. TSA based the validator requirements in this IFR, in part, on the UK program. In both programs, entities wishing to serve as validators seek approval from the government regulatory agency. In both programs, the government reviews the validators' assessments and, where appropriate, government agents may conduct inspections to determine if enforcement action is necessary.

In addition to these structural similarities, some of the methods to secure cargo will be similar in the two programs. For example, the UK program makes use of tamper-resistant seals, tamper evident tape, and procedures to document that the cargo is not subject to unauthorized access from the time the cargo is screened until it is tendered to an aircraft operator for transport on a passenger aircraft. These are key elements in the CCSP "chain of custody" framework.

The UK program has been in place since 2003 and has achieved the benefits TSA seeks to gain from the CCSP. Known consignors screen close to 50 percent of cargo that otherwise would be screened by aircraft operators and foreign air carriers on airports; the rest of the cargo is screened by air carriers. Having aircraft operators and foreign air

carriers screen all cargo at airports could result in delays in flights and backlogs of cargo to be screened. The UK program significantly reduces potential adverse impacts on the flow of commerce that otherwise could result if aircraft operators and foreign air carriers were required to screen all cargo. The same concerns exist for screening cargo at U.S. airports.

D. Certified Cargo Screening Pilot Programs

TSA is testing the concept of screening earlier in the supply chain by conducting two parallel pilot programs: (1) the CCSP pilot involving shippers and other entities, such as manufacturers, distributors, and third party logistics companies, and (2) the IAC technology pilot. The CCSP pilots began at the following major gateway airports representing over 65% of all air cargo loaded on passenger flights: San Francisco (SFO), Chicago (ORD), Philadelphia (PHL), Seattle (SEA), Los Angeles (LAX), Dallas-Fort Worth (DFW), Miami (MIA), Atlanta (ATL), and New York/Newark (JFK/EWR). The IAC pilot is now in effect at all U.S. airports.

Over 65 percent of all cargo transported on passenger aircraft is carried on wide-body passenger aircraft, such as a B-767, from the airports listed above. Approximately 43 percent of cargo transported on wide-body aircraft originates in 6 of these airports. Thus, TSA focused its outreach for the pilot programs on the entities using the airports with the highest volume of cargo transported on wide body passenger aircraft. Industry agreed to participate in the pilots.

TSA conducted outreach for the CCSP pilot program by contacting 120 shippers and other entities in 9 major cities. The CCSP pilot focuses on the ability of these entities to screen cargo according to methods approved by TSA, primarily by physical search of

the shipping box before it is closed, sealed, and leaves the facility using a secure chain of custody. Shippers, manufacturers, distributors, and third-party logistics companies are in the best position to screen the contents of the box before it leaves their facility, as they know what should be in the box and can spot anomalies quickly. As long as the screening is conducted in accordance with TSA procedures and the chain of custody remains intact when the cargo is loaded on passenger aircraft, the cargo does not have to be rescreened.

The IAC technology pilot is evaluating the effectiveness of cargo screening technology and processes recommended by TSA by commodity class at each participant's consolidation facility. Congressional appropriations provided TSA with funds for the screening of air cargo. TSA is using these funds in part to assist in the deployment of appropriate screening technology for use in the IAC pilot. The IAC technology pilot participants must use either x-ray or Explosive Trace Detection (ETD) equipment during the screening process. This pilot is also evaluating the IAC community's ability to screen cargo volumes, and the use of chain of custody procedures.

When the IFR becomes effective, the CCSP pilot program will end. Participants will become CCSFs under the IFR. The IACs in the IAC technology pilot will continue to collect and submit information to TSA regarding the cargo screening technology until August, 2010. TSA will collect information after the IFR becomes effective under OMB's Paperwork Reduction Act approval for the IFR; this information will include the data collected during the IAC technology pilot. After the completion of the IAC technology pilot, DHS will conduct an evaluation of the pilot.

III. TSA's Program for Achieving the Statutory Mandates for Cargo Loaded Domestically

With respect to cargo loaded within the United States, TSA implemented two measures that assisted industry in achieving the requirement that 50 percent of cargo transported on passenger aircraft be screened by February 3, 2009. First, on August 1, 2008, TSA issued an amendment to the Aircraft Operator Standard Security Program that requires 100 percent screening of cargo transported on narrow-body passenger aircraft. Narrow-body aircraft represent 96 percent of all domestic passenger flights, and approximately one-quarter of all cargo on passenger aircraft travels on narrow-body aircraft. TSA has required that all cargo on narrow-body passenger aircraft, such as a B-737, must be screened. This requirement was a key component of achieving the 9/11 Act's requirement to ensure that 50 percent of cargo on passenger aircraft was screened by February 2009. The second key component was to have IACs participating in the pilot program at the major gateway airports screen cargo prior to their consolidating the cargo for the airlines. Data from the pilot programs, as well as inspections by TSA Inspectors, demonstrates that industry has achieved the 50 percent milestone of the 9/11 Act.

This rule is a key component of our strategy to maintain 50 percent screening as of February 3, 2009, and to achieve 100 percent screening by August 3, 2010. The rule will allow shippers to screen their cargo prior to tendering it to the airlines. We have developed this IFR implementing the permanent CCSP based on lessons learned in the CCSP pilot program. We estimate that, at full implementation, certified cargo screening

facilities and aircraft operators will screen cargo traveling on passenger aircraft as follows:

- Of the 4.3 billion pounds of cargo shipped on passenger aircraft annually, aircraft operators will screen 30 percent of the cargo or 1.3 billion pounds;
- CCSFs using screening equipment will screen 38 percent of the cargo or 1.6 billion pounds; and
- CCSFs using physical search methods to screen will screen 32 percent of the cargo or 1.4 billion pounds.

IV. Organization of the Rule

The section-by-section analysis below is organized sequentially to follow the CFR numbering. This rule amends a number of TSA's existing regulations and adds several new parts to the CFR. Briefly, these changes include the following:

- The rule expands 49 CFR part 1515 to provide redress procedures for individuals who undergo STAs in connection with their air cargo work for aircraft operators, certified cargo screening facilities, and validation firms, if they receive an adverse decision from TSA.
- The rule amends 49 CFR part 1520, the regulations governing sensitive security information (SSI), requiring these newly-regulated populations, such as CCSFs and validators, to protect such information from disclosure.
- The rule adds a new 49 CFR part 1522, establishing a system to authorize TSA-approved validators to perform assessments of CCSFs. It also provides a framework for potential future use in other TSA programs.

- The rule amends the existing STA regulations in 49 CFR part 1540, subpart C, to encompass newly-required STAs for certain personnel of certified cargo screening facilities and approved validation firms. Also, the rule amends the list of biographic information that applicants and operators must provide TSA, so that TSA can conduct more efficient threat assessments. In addition, the rule adds provisions to facilitate the use of comparable threat assessments in place of the assessments that TSA requires in subpart C of part 1540.
- The rule amends 49 CFR parts 1544 and 1546 to impose new requirements on U.S. aircraft operators and foreign air carriers with respect to the cargo screening and acceptance of cargo from CCSFs.
- The rule also amends 49 CFR parts 1544, 1546, and 1548 to clarify which individuals are subject to the STA requirements and to better reflect current TSA requirements in the standard security programs for U.S. aircraft operators, foreign air carriers, and IACs.
- The rule adds a new 49 CFR part 1549, which provides the regulatory requirements for facilities participating in the CCSP. Requirements include qualifications of screening personnel, STAs, adoption of security programs, and cargo screening procedures.

V. Section-by-Section Analysis

Part 1515—Appeal and Waiver Procedures for Security Threat Assessments for Individuals

Section 1515.1-Scope

In part 1515, TSA sets forth redress procedures for many of the transportation workers who must successfully complete an STA. These STAs are described more fully in the Section-by-Section analysis for part 1540, subpart C. The redress procedures include administrative appeals, requests for waivers, and review of certain cases by administrative law judges. This rule amends § 1515.1 to expand the scope of part 1515 to include applicants engaged in air cargo operations who work for certified cargo screening facilities or validation firms who have applied for an STA and wish to appeal an Initial Determination of Threat Assessment or an Initial Determination of Threat Assessment and Immediate Revocation.

Section 1515.9-Appeal of Security Threat Assessment Based on Other Analyses

This rule revises §1515.9 to expand its scope to allow applicants engaged in air cargo operations who work for certified cargo screening facilities or validation firms to appeal an Initial Determination of Threat Assessment in which TSA has determined that the applicants pose a security threat under 49 CFR 1549.107.

Section 1515.11-Review by Administrative Law Judge and TSA Final Decision Maker

This rule revises §1515.11 to allow applicants engaged in air cargo operations who work for certified cargo screening facilities or validation firms and who have received Final Determinations of Threat Assessment after appeals as described in

§ 1515.9 to obtain review of these determinations by an administrative law judge and the TSA Final Decision Maker.

Part 1520—Protection of Sensitive Security Information

Implementation of this rule will create new types of sensitive security information (SSI) and new populations of persons with access to, and responsibilities for, protecting all SSI. See Footnote 1. Therefore, TSA is making the following changes to part 1520, which implements the SSI program.

Section 1520.5-Sensitive Security Information

This rule amends the list of information constituting SSI in § 1520.5 to include the SSI to be created under this rule. Specifically, TSA adds "air cargo" to paragraph (b)(1)(i) of this section, which contains the listing of security programs that constitute SSI. Such programs include those for IACs as well as for CCSFs and validation firms. TSA has determined that validation firm security programs (operating under part 1522) and CCSF security programs (operating under part 1549) to be SSI because they will contain specific information about how the operation will implement measures for personnel security, physical security, chain-of-custody controls, and other measures that—if publicly disclosed—would allow a terrorist or other person with malicious intent to jeopardize air cargo security.

In a related, clarifying change, this rule amends § 1520.3 to remove the definition of "security program." This definition, which is only used in § 1520.5, is unnecessary, because it only describes which security programs are SSI, a subject which is entirely covered in § 1520.5. Removing this duplicative provision will preclude possible confusion. TSA moved the phrase "including any comments, instructions, or

implementing guidance" from the definition of security program to § 1520.5(b)(1) to make clear that comments, instructions, and implementing guidance for security programs are protected in the same way as the security programs themselves.

Section 1520.7-Covered Persons

This rule also amends the definition of "covered person" in § 1520.7 to include personnel of certified cargo screening facilities and of validation firms. These persons will have access to SSI, including security programs and applicable security directives and orders. Including these persons as "covered individuals" brings them within the scope of the responsibilities for protecting SSI that are contained in 49 CFR 1520.9. These include the duty to protect SSI from disclosure and to report incidents of unauthorized disclosure to TSA.

Part 1522—TSA-Approved Validation Firms and Validators

The provisions of part 1522 establish a system in which TSA approves validation firms; these firms are responsible for hiring individuals, called validators, who must have specific qualifications. These validators are responsible for conducting the assessments of the facility seeking certification or recertification as a CCSF operating under part 1549. The CCSF applicants (whether they are individual companies or IACs) will pay the validation firm for the validation assessment. TSA will not charge or establish a fee for that purpose.

Firms that seek to perform the functions of validation firms for purposes of the CCSP must apply to TSA for approval and, once approved, must perform the functions in accordance with TSA's requirements. The criteria for approval and the performance requirements are set forth in part 1522 and described below. Part 1522 also addresses the

qualifications and responsibilities of individual validators, who, on behalf of a validation firm, actually perform the assessments of persons, operations, or facilities regulated under this chapter.

Section 1522.1-Scope and Terms Used in this Part

Section 1522.1(a) explains that part 1522 governs the use of private firms employing individual validators to assess whether certain persons regulated by TSA are complying with security programs applicable to those persons and other TSA requirements.

Paragraph (b) of § 1522.1 defines the terms used in part 1522. The rule defines "TSA-approved validation firm" or "validation firm" as a firm that has received TSA's approval to make such assessments on whether regulated persons have complied with security programs and other TSA requirements applicable to those persons. The rule defines "applicant" as a firm seeking to become a TSA-approved validation firm. The rule's definition of "firm" includes business enterprises, including individuals operating as a business, as well as other non-governmental organizations, such as non-profit corporations. The term "validator" means the particular individual assigned by the validation firm to perform a given assessment; thus, the terms "validation firm" and "validator" are not synonymous. The term "assessment" as defined in § 1522.1, refers to the validator's evaluation of compliance with the relevant requirements of a security program.

The rule also defines the term "national of the United States." For purposes of this rule, 'national' 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. It is consistent with the definition of the same term (49 CFR 1570.3) in the Maritime and Land Transportation Security regulations and with the definition in 8 U.S.C. 1101(a)(22).

Validation firms and validators must be free of conflicts of interest to perform assessments for TSA programs. Section 1522.129(a) requires validation firms to maintain records demonstrating compliance with this regulation, including the conflict-of-interest requirements. As part of the inspection process, TSA may review records concerning a facility's compliance with conflict of interest provisions.

Section 1522.1(b) defines "conflict of interest" as a situation in which a relationship with, or a financial interest in, the person being assessed may adversely affect the impartiality of the assessment. This definition encompasses the validation firm as an entity, as well as the individuals of the firm who will be conducting, or assisting in conducting, the assessment, and their immediate family members. This definition is derived in part from the Government Auditing Standards established by the Government Accountability Office (GAO) for ensuring that Government auditors or their employees do not have business or personal impairments that would interfere with their ability to maintain their independence. See GAO, Government Auditing Standards (July 2007), ch. 3. The definition is also derived, in part, from the post-governmental employment restrictions applicable to Federal employees.

The definition of "conflict of interest" in § 1522.1(b) contains several examples. It includes examples of conflict-of-interest situations applicable to a validation firm as an entity, such as parent-subsidiary relationships and common management or organizational governance (for example, interlocking boards of directors). It also

includes an example of a conflict of interest situation in which the validation firm, or validator, or the individual assisting the validator, or his or her immediate family member as an individual, is a creditor or debtor of the person being assessed. It also lists examples of conflicts of interest related to financial interests, such as investments in debt and equity, in the person being assessed.

The other examples of conflict of interest in the definition address situations in which the validator or an individual assisting the validator, or his or her immediate family member, is a former employee, officer, or contractor including a consultant of the person being assessed. If the former duties and responsibilities of the validator or individual assisting the validator involved the operations or functions to be assessed, he or she has a permanent conflict of interest; such an individual may never conduct or assist in conducting an assessment of an operation or function with respect to which he or she had duties or responsibilities. If the former duties and responsibilities of the validator or individual assisting the validator did not involve the operations or functions to be assessed, he or she must observe a two-year "cooling-off period" during which he or she may not conduct assessments of his or her former employer. These concepts are consistent with the post-employment restrictions applicable to governmental employees found at 18 U.S.C. 207. Individuals who are former employees of the person being assessed who will not be conducting or assisting in the assessment do not create a conflict of interest if they are segregated from the assessment work.

Section 1522.3-Fraud and Intentional Falsification of Records

Section 1522.3 includes provisions that prohibit any person, whether the validation firm, the validator, or another individual, from making or providing any

fraudulent or intentionally false statements, reports, records, access mediums, or identification. The same prohibitions apply to persons regulated under TSA's Civil Aviation Security regulations; see 49 CFR 1540.103, on which this section is based. Any intentional falsification or fraud may constitute a basis for TSA to withdraw the validator's approval. In addition, any intentional falsification or fraud may constitute a violation of certain criminal laws such as 18 U.S.C. 1001. In appropriate cases TSA will refer potential criminal violations to the U.S. Attorney for investigation.

Section 1522.5-TSA Inspection Authority

Section 1522.5 sets out TSA's broad authority to inspect a validation firm and a validator, including on-site inspections and the copying of records. TSA needs such broad authority to perform its role in monitoring compliance with this part. Paragraph (a) requires each validation firm to allow TSA to enter the facility to make inspections or tests, including copying records. A validation firm's operations are unlikely to give rise to the kinds of emergencies that would require after-hours inspections, so this paragraph only refers to TSA inspections during normal business hours. This paragraph also provides that the inspection may be without advance notice. While TSA expects often to provide advance notice of an inspection, we must have the ability to do so unannounced to verify compliance by the validation firm and its personnel and to otherwise assess security. The inspections referred to in paragraph (a) include inspections for compliance with the statute and TSA rules, and includes inspections that TSA may make to carry out duties assigned to TSA in 49 U.S.C. 114(f), as set out in § 1522.5(a)(2).

Section 1522.5(b) provides that at the request of TSA each validation firm and validator must provide evidence of compliance with the TSA regulations, which are

located in 49 CFR chapter XII, including parts 1500-1699. This may include providing records to TSA or other evidence to show compliance. Paragraph (c) provides that TSA and DHS officials working with TSA may conduct inspections without access media issued or approved by a validation firm or other person. This is to facilitate the inspection process and make it possible for TSA to conduct unannounced inspections. It is based on a similar provision in § 1542.5(e) that applies to airport operators. Taken as a whole, this section will allow TSA to evaluate the validation firm's and the validator's respective performance, and to evaluate the reliability of the validator's assessments.

Section 1522.101-Applicability

Subpart B, which begins at § 1522.101, applies specifically to the use of TSA-approved validation firms and validators in the context of the CCSP. Each facility that seeks to be a CCSF will need to engage a validation firm to assess whether that facility complies with the security program that TSA requires under 49 CFR 1549.5.

Section 1522.103-Requirements for Validation Firms

Section 1522.103 establishes the general requirements for validation firms. Paragraph (a) states the fundamental requirement, which is that the firm must have the necessary facilities, resources, and personnel to conduct assessments. Among other things, this requirement entails the demonstrated capability to define, execute, and document standardized business processes. The validation firm must also demonstrate its capability to hire and train personnel to perform operations similar to the assessments required under this subpart and part 1549. The purpose of this requirement is to establish a basis on which TSA may evaluate whether a firm has the experience and capabilities to perform as a validation firm.

Paragraph (b) provides that each validation firm must have a Security Coordinator and one or more alternates. This provision is based on the concept of Security Coordinator for IACs as implemented in 49 CFR 1548.13. These individuals must be senior officers or employees to ensure that they have the authority necessary to fulfill their functions. They serve as the validation firm's primary point of contact with TSA on security-related matters. Because a validation firm has a support (as opposed to an operational) role in the certified cargo security program, the Security Coordinator or an alternate must be available during regular business hours (rather than on a 24-hour basis). Also, the Security Coordinator and alternates bear the responsibility of immediately initiating corrective action if the firm discovers an instance of non-compliance with any applicable TSA security requirement. These requirements ensure that each validation firm has at least one readily available and accountable individual with adequate authority to monitor security-related matters.

Under paragraph (c) of § 1522.103, the validation firm must hold and carry out a TSA-approved security program. This topic is covered in more detail in the discussion of § 1522.105, below.

Paragraph (d) of § 1522.103 imposes an affirmative obligation on the validation firm to ensure that its personnel carry out the requirements of TSA's regulations and the security program. "Personnel" includes direct employees, contractors, agents, and other persons acting on behalf of the validation firm.

Finally, paragraph (e) requires the validation firm to notify TSA of all pertinent changes in information that the validation firm must submit to TSA. Examples of such information include changes of address, changes in the identity of the Security

Coordinator or alternates, and significant changes in the ownership of the firm. A significant change in the ownership would include, for example, acquisition of the firm by another business entity, or the form of the firm's organization, for example, incorporation. It would not include a minor change in the identity of shareholders.

Section 1522.105-Adoption and Implementation of the Security Program

Paragraph (a) of § 1522.105 provides that a validation firm must hold and carry out an approved security program in order to operate as a validation firm. Paragraph (b) outlines the requirements for the content of the validation firm standard security program. These requirements are generally consistent with the similar requirement for IACs in part 1548.

Paragraph (b)(1) states the fundamental purpose of the security program, which is to provide for the security of aircraft and protect against threats to air security. Paragraph (b)(1) thus establishes that validation firms, even though they serve a supporting role, are important components in the overall certified cargo security program.

Key among these requirements for security programs is that the programs must specify the processes and procedures that the firm will use to maintain the qualifications of its validators and its personnel assisting validators with assessments. This is important, because the quality of the validation firm's operational performance depends primarily on the expertise of its personnel, especially the validators. Thus, the security program must describe in detail how the validation firm will maintain the current qualifications, accreditations, credentials, training, and STAs for its relevant personnel.

The security program must also include provisions for a Security Coordinator, as well as for setting managerial responsibilities for ensuring that the firm's personnel carry out their responsibilities under TSA regulations and the security program.

Paragraph (c) of § 1522.105 sets out procedures by which an applicant or a validation firm may request amendments to a security program. Paragraph (d) sets out the process by which TSA will initiate amendment of a security program. Paragraph (e) covers emergency amendments, which TSA may make without prior notice and which take effect immediately. The provisions of paragraphs (c), (d), and (e) are analogous to similar provisions relating to IAC security programs (49 CFR 1548.7), which provides that TSA may issue emergency amendments to aircraft operators if there is an emergency requiring immediate action with respect to safety in air transportation or in air commerce that makes procedures in § 1522.105 contrary to the public interest; such provisions establish an orderly process for revising security programs when circumstances change. Similar provisions exist in 49 CFR 1542.105(d) (airport operators), 1544.105(d) (aircraft operators), 1546.105(d) (foreign air carriers), and 1548.7(e) (indirect air carriers). Paragraph (f), parallel with 49 CFR 1548.5(d), provides basic requirements on availability of the security program to the firm's personnel and to TSA and requires measures to protect it as SSI.

Section 1522.107-Application

Section 1522.107 sets out the procedures by which a firm may apply for approval to operate as a validation firm. TSA will prescribe the form and manner of the application, which must be in writing and submitted at least 90 days in advance.

Paragraph (a) enumerates the required items that applicants must include in their applications. Among other items, applicants must include a statement declaring whether the applicant is a small business; the collection of this information assists TSA in developing appropriate civil penalty formulas.

Paragraph (b) of § 1522.107 discusses the next step in the application process. After TSA receives the initial application specified in paragraph (a), and after the applicant's Security Coordinator has successfully completed a STA, TSA will send the validation firm, via the Security Coordinator, a copy of the Validation Firm Standard Security Program. TSA anticipates that all information will be sent to participants via electronic means in a password protected mode. TSA also plans to develop a secure web address that will be available to the participating validation firms to obtain copies of the security program. The validation firm must also submit a supplement to its security plan 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. This provision establishes a baseline of standardization, while allowing for flexibility in appropriate circumstances. TSA will seek comment on the validation firm security program from applicants as part of the application process. Thereafter, any approved validation firm may request amendments to its security program.

Section 1522.109-TSA Review and Approval

Paragraph (a) of § 1522.109 lists the criteria that TSA will employ in reviewing an application submitted under § 1522.107. As provided in paragraph (b), TSA will approve or disapprove the application based on these criteria. In either case, TSA will

provide written notice to the applicant. In the case of an approval, TSA may approve or require modifications to the security program applicable to the applicant. The validation firm will also demonstrate to TSA how the validators employed by the firm will meet TSA qualifications. In the case of a disapproval, TSA will state the basis for the disapproval in writing.

Under paragraphs (b)(1) and (2), a validation firm may commence operations only after it receives approval of its security program and approval to operate as a validation firm, and after the relevant personnel have completed all required training and STAs. These paragraphs make it clear that the validation firm must satisfy all of these elements before the validation firm may conduct assessments.

As provided in paragraph (c), the duration of an approval granted under this section is 12 months.

The following table demonstrates the certification and training cycles for CCSFs and validation firms.

	IAC Operating Certificate (Renewal Application)	Validation Firm Operating Approval	Certification	Recurrent Training
Shipper/CCSF	N/A	N/A	Every three years	Annually
IAC/CCSF	Annually	N/A	Every three years	Annually
Validation Firm/Validator	N/A	Annually	N/A	Annually

Section 1522.111-Reconsideration of Disapproval of an Application

Section 1522.111 describes the review and petition process for TSA's reconsideration of disapproval of the validator's application. If an applicant challenges the disapproval, the applicant must submit a written petition for reconsideration within 30 days of receipt of the notice of disapproval. The petition must include a statement, with supporting documentation, explaining why the applicant believes the application meets the criteria of § 1522.103. Reconsideration may result in confirmation of the disapproval or in an approval. Disposition pursuant to this section constitutes a final agency action for purposes of review under 49 U.S.C. 46110.

Section 1522.113-Withdrawal of Approval

Section 1522.113 establishes procedures by which TSA may withdraw a previously-granted approval of a validation firm. This may occur if the validation firm no longer meets the qualification standards, if the validation firm fails to conduct assessments in compliance with TSA's requirements, or if withdrawal is in the interest of security or the public. 49 CFR 1522.113(a). If TSA withdraws a validation firm's approval, the validation firm must immediately stop performing any and all activities related to assessments. In determining whether withdrawal is appropriate, TSA considers the number, frequency, and severity of security violations committed by a regulated party. If TSA determines withdrawal is appropriate, TSA will remove the validation firm from the list of approved validation firms.

Under paragraph (b) of § 1522.113, TSA will provide the validation firm with a written notice of proposed withdrawal of approval that will include a statement of the basis for the proposed withdrawal of approval. Paragraph (c) provides for immediate

withdrawal of approval in emergency circumstances. Upon receipt of a notice of emergency withdrawal under paragraph (c), the validation firm must immediately stop performing assessments, and must discontinue any assessments in progress. Paragraphs (d) and (e) provide a reconsideration procedure that may result in confirmation of the withdrawal of approval or in a decision to allow the validation to retain (or regain) its approval. Disposition pursuant to this section is constitutes a final agency action for purposes of review under 49 USC. 46110.

Section 1522.115-Review of TSA Approval

It is important that validation firms meet TSA's standards both before and after they begin performing validations. TSA will actively monitor validations through a process of initial and recurrent reviews. Approved validation firms must apply for renewal of approval annually. During these reviews, TSA will examine, among other things, whether the validation firm's personnel have received required training and whether the relevant personnel have maintained the required accreditations and/or certifications. The review will also focus on the firm's compliance with part 1522 and with its security program.

Section 1522.117-Qualifications for Validators

Section 1522.117 prescribes the necessary qualifications for individuals selected by validation firms to serve as validators for particular assessments. The requirements establish minimum levels of expertise and experience that an individual must have before he or she may be employed as a validator. As explained in the discussion of § 1522.123 below, a properly qualified validator must be directly responsible for the conduct of each assessment. A validation firm may assign an individual to be a validator with direct

responsibility for an assessment only if the individual meets the qualifications specified in § 1522.117(a)(1)-(5) described below. The validation firm will be responsible for determining whether an individual has the appropriate qualifications to serve as a validator, and TSA will inspect for compliance with these requirements.

Pursuant to paragraph (a)(1) of § 1522.117, an individual must be a U.S. citizen or national, or be an alien lawfully admitted to the United States as a Lawful Permanent Resident (LPR) in order to function as a validator. For aliens to become LPRs (commonly referred to as "green card" holders), the U.S. Government must have determined that they are admissible to the United States as immigrants; that determination requires security and criminal checks. TSA will allow LPRs to function as validators based on the fact that the U.S. Government has already performed security and criminal checks on these individuals.

Validators must have extensive experience in conducting assessments, inspections, or audits before undertaking duties under this part. Paragraph (a)(2) identifies two bases on which individuals can establish they possess the appropriate level of experience. Under the first basis, he or she must have an accreditation or certification from an organization that TSA recognizes as qualified to certify or accredit a validator assessing facilities, such as certified cargo screening facilities, or the individual must have five years or more experience in conducting inspections under State or Federal regulatory programs in the security industry, the aviation industry, or other government programs. TSA will review the accreditation of a validator when the validation firm submits a plan to TSA demonstrating how the firm will ensure that the validators in the firm meet TSA qualifications. If a validator does not meet the accreditation standards,

TSA may deny approval to the validation firm or may approve the firm but direct that the individual without the necessary accreditation not be used for the CCSP program.

Examples of an organization qualified to accredit a validator would include the International Standards Organization and ASIS International. TSA will make publicly available on the TSA public web site a list of acceptable accreditation or certification organizations. The individual must have had this experience within the past ten years. Under the second basis, he or she must show relevant experience and expertise by having been employed by a Federal or state government agency as an inspector, assessor, or auditor in assessment or inspection tasks similar to the assessments under this part. Inspectors for governmental agencies receive thorough training and are subject to rigorous qualification standards. For example, a former Department of Transportation safety inspector would presumably have this kind of experience.

Under paragraph (a)(3), the individual must have three current professional references. The purpose of this requirement, which is related to the requirements of paragraph (a)(2), is to allow the validation firm and TSA to further verify the experience and expertise of the validator.

The expertise and experience of the validators is a critical component of this program. Paragraph (a)(4) states the requirement that validators must understand the requirements of the program in order to perform their functions. A validation firm must be able to demonstrate that each of its validators has this understanding. Although a validator's successful completion of the training required in § 1522.119 will demonstrate initial understanding, a validator must also demonstrate the necessary knowledge and its practical application when the validator conducts assessments under this program.

Section 1522.119-Training

As stated above, validators must understand the requirements of the program and applicable technologies and practices before they begin conducting assessments. The validation firm must ensure that all employees associated with the assessment process complete training to ensure that they are capable of effective performance of their duties, and are knowledgeable about their security responsibilities. This is consistent with training requirements in other TSA regulatory programs. TSA plans to make a training program available for the validation firms. As program requirements change and technologies and practices improve, validators will need to keep up-to-date. Therefore, § 1522.119 requires validators and other individuals who assist in conducting assessments to complete initial and annual recurrent training provided by TSA. Under § 1522.119(a), the relevant individuals must complete initial TSA training on the standards, procedures, and forms prescribed by TSA for assessments of a CCSF before undertaking an assessment under subpart B. Under § 1522.119(b), validators and other relevant individuals must complete annual training; the training will include current information and will confirm that the validators and other individuals have maintained the necessary expertise to continue to perform assessments. Paragraph (c) outlines the general requirements for the content of the training; this outline is not exhaustive. Section 1522.119(c) provides that the "training required by this section will include coverage of the applicable provisions of this chapter, including this part, part 1520, and section 1540.105." (Part 1520 covers Sensitive Security Information (SSI), and § 1540.105 covers security responsibilities of employees and other persons.) TSA intends to specify more detailed training requirements in the applicable security programs.

Section 1522.121-Security Threat Assessments for Personnel of TSA-Approved Validators

This section requires individuals supervising, performing, or assisting in the performance of validation assessments, and the validation firm's Security Coordinator and alternates, to successfully undergo a STA conducted by TSA under 49 CFR part 1540, subpart C, or an STA that TSA deems comparable. See the discussion of 49 CFR part 1540, subpart C for a full description of those requirements.

Section 1522.123-Conduct of Assessments

Section 1522.123(a) establishes the general rule that a validator must conduct each assessment of a CCSF under this part in a form and manner to be prescribed by TSA. The provision will increase the standardization of assessments across the program, promoting security and fairness. While other individuals may assist a validator, the validator must be directly responsible for the assessment and must sign the assessment report required by part 1522. This provision emphasizes the authority and accountability of the validator within the overall regulatory scheme.

Section 1522.123(b) provides that validators may not undertake an assessment in which the validator, the validation firm for which he or she works, or any other individual who would work on the assessment, has a conflict of interest as defined in § 1522.1.

Section 1522.123(c) applies when a validator, while conducting an assessment, learns that there is or may be an instance of noncompliance with TSA's requirements that presents an imminent threat to transportation security or public safety. In such a situation, the validator must report the noncompliance to TSA, through the Security

Coordinator immediately. The purpose of this provision is to allow TSA the opportunity to address and correct potentially dangerous situations promptly.

Section 1522.123(d) provides that neither a validation firm nor a validator may require the CCSF being assessed to take remedial action. While a validator may suggest "on the spot" remedial actions in the course of conducting an assessment, the validator does not have the authority to require such remedial action. The validator will, of course, include in the report to TSA any matters that he or she believes are not in compliance with TSA requirements. The rule also clarifies that the validation firm and validator may not take disciplinary or enforcement action against a facility it has assessed. Only TSA may take disciplinary action against the CCSF. If the validator reports non-compliance, TSA will evaluate all the facts and circumstances, likely will conduct an inspection, and determine whether to take action.

Section 1522.123(e) provides that a validator must not conduct more than two consecutive assessments of a given facility seeking approval, or renewal of approval, to operate a CCSF. Under § 1549.7(b) each CCSF must apply for renewal every three years. Thus, if a validator has conducted the initial assessment and the first renewal assessment, or two consecutive renewal assessments, for a given CCSF, that validator may not conduct the next assessment on that CCSF. The purposes of this requirement are to maximize the objectivity of the validator and to assure a fresh assessment for each CCSF every few years.

Section 1522.125-Protection of Information

Section 1522.125(a) specifies that validation firms must comply with TSA's regulations (49 CFR part 1520) for identifying, handling, and protecting SSI. Under

paragraph (b) of § 1522.125, validation firms may not disclose any proprietary information that is disclosed to the validator during the assessment. This provision is intended to protect the facilities being assessed and to encourage their full cooperation with the validators.

Section 1522.127-Assessment Report

Section 1522.127 requires a validator to prepare an assessment report that must include information about the assessment process and the validator's assessment of the CCSF's compliance with applicable TSA requirements. The validator must submit the assessment report within 30 days after completing the assessment. The validator must attest that he or she performed the assessment professionally and impartially. TSA will use the assessment report to determine whether additional TSA action, such as further inspection by TSA personnel, is required. The assessment report must contain the information specified in § 1522.127(b).

Section 1522.129-Recordkeeping Requirements

Section 1522.129(a) requires validation firms to maintain records demonstrating compliance. Paragraph (b) requires the firms to retain records pertaining to individuals, including training, STAs, and qualification of validators (including conflicts of interest), until the 180th day after the individual leaves the employment of the validation firm. The retention period parallels the record retention requirements related to STAs under part 1540.

Paragraph (c) covers records about the validation firms' approvals from TSA, which each validation firm must retain until completion of the validation firm's next

review under § 1522.115. This retention period should help ensure that TSA has the necessary documentation with which to complete the review.

Paragraph (d) covers assessment reports and back-up documentation, which includes working papers and interview notes, pertaining to particular assessments conducted by the validation firm. Validation firms must retain records covered under this paragraph for 42 months after completion of the assessment. This retention period should assure that the materials will be available at least until the CCSF's next recertification.

With respect to each of the record retention periods specified in § 1522.129, the validation firm may destroy a record upon the expiration of the period, unless TSA instructs the firm to retain the record longer.

Part 1540—Civil Aviation Security: General Rules

Section 1540.5-Terms Used in this Subchapter

This rule amends § 1540.5 to add definitions of the terms ''certified cargo screening program" and "certified cargo screening facility." "Certified cargo screening program" means the program, established under 49 CFR part 1549, under which TSA authorizes facilities to screen cargo to be offered for transport on certain passenger aircraft. A "certified cargo screening facility" is a facility that TSA certifies to screen this cargo and perform the other functions required by part 1549. As used in this chapter, "certified cargo screening facility" refers to the legal entity that operates a CCSF at a particular location.

Part 1540—Civil Aviation Security: General Rules

Subpart C-Security Threat Assessments

This subpart covers the STAs that are required throughout the aviation security rules, including those for certain aircraft operator, foreign air carrier, and IAC personnel. This rule expands the subpart to include CCSF and TSA-approved validation firm personnel.

The STA process works as follows. First, the CCSF employee submits the biographic data for their STA application through secure, web-based tool. Required biographic data includes:

- legal name;
- current mailing address;
- gender;
- date and place of birth;
- social security number;
- citizenship status;
- alien registration number if employee is not a U.S. citizen;
- daytime phone number; and
- name, address, and telephone number of individual's employer.

Next, TSA sends the STA application data to an automated vetting engine where a name-based terrorism check is performed. The name-based terrorism check consists of matching against the Terrorist Screening Database (TSDB), which includes the No-fly list and Selectee list.

If TSA determines that the individual poses a security threat, TSA issues an Initial Determination of Threat Assessment (IDTA) to the individual. The determination includes a statement that explains why TSA believes the individual is not eligible or may pose a security threat and the process by which the individual may appeal the determination. All STA results, favorable or unfavorable, are communicated to the CCSF though the TSNM STA Tool.

Section 1540.201-Applicability and Terms Used in This Subpart

This rule amends § 1540.201 to provide that the STA requirements in subpart C on part 1540 "Security Threat Assessments" now apply to validation firms and facilities participating in the CCSP. Paragraphs (a)(6) through (a)(12) list persons who must comply with this subpart, which includes entities that are subject to the subpart and the specific individuals in the CCSP who must undergo STAs in accordance with subpart C:

- Each CCSF;
- Individuals at CCSFs performing or supervising screening;
- Individuals at CCSFs with unescorted access to screened cargo;
- The senior manager or representative in control of the operations of a CCSF;
- Employees of validation firms supervising, performing, or assisting in validations under 49 CFR part 1522; and
- Security coordinators and alternates of certified cargo screening facilities and validation firms.

These individuals must successfully complete STAs, because they will have unescorted access to cargo and, thus, the opportunity to compromise the security and safety of the process. In this rule, TSA requires these individuals to complete the name-

based check of relevant domestic and international watch lists, which also includes a limited immigration check. In the future, TSA may propose rules to require these individuals to also complete a fingerprint-based criminal history records check (CHRC) and a more thorough immigration status check. However, TSA has not yet developed the enrollment system necessary to gather fingerprints from these applicants. These individuals play important roles in securing cargo transported on certain passenger aircraft and would have the opportunity to contaminate cargo if they so desired. Therefore, it is critical that TSA vet them to determine whether they may pose a threat to national or transportation security before allowing them access to the cargo screening system.

TSA is also expanding the definition of "operator" in paragraph (b) to include CCSFs and validators.

Section 1540.203-Security Threat Assessment

We revise § 1540.203(a) to include the new individuals who must successfully complete an STA, listed above in §§ 1540.201(a)(6)-(12).

We revise the identity and work authorization requirements in paragraph (b) of this section. Former paragraph (b) required operators to authenticate an applicant's identity by reviewing two forms of identification, one of which must be a government-issued picture identification. Amended paragraph (b) requires operators to verify the identity and work authorization of each applicant by examining standard identity and work authorization documents and examine the documents to determine whether they appear to be genuine and relate to the applicant presenting them. TSA recommends that operators use the identity and work authorization documents approved for such use by the

U.S. Citizenship and Immigration Services (USCIS) in the "Form I-9, Employment Eligibility Verification, List of Acceptable Documents" to meet the identity and work authorization verification. See www.uscis.gov/files/form/I-9.pdf for the most current list of documents approved by USCIS for identity and work authorization verification. Also, we now require operators to retain a copy of the document(s) used to verify identity and work authorization for at least 180 calendar days after the applicant is no longer employed by the operator. 49 CFR 1540.201(d). This will enable to TSA to conduct periodic document inspections to verify that operators are satisfying the requirements.

Identity verification and confirmation that an individual is authorized to work in the United States are critical steps in the STA process. If an individual presents fraudulent documents with an incorrect name, date of birth, country of citizenship, or other data, TSA's STA will be flawed at inception. Companies with more sophisticated personnel systems may opt to scan the identity and work authorization documents electronically and use fraud detection software to "score" the documents for authenticity. These software programs are becoming economically and operationally desirable as a standard process in many industries, and TSA uses these systems in other vetting programs where TSA is responsible for enrolling applicants.

Paragraph (c) of this section describes the information operators must collect from applicants and transmit to TSA for the STA. The rule amends this list in some respects to ensure that we have the best information on which to base an accurate STA and that TSA can easily contact the applicant if we need to resolve incomplete or conflicting information. The rule now requires submission of the applicant's daytime phone number and the name, address, and telephone number of the applicant's employer. TSA has

found that this information is very helpful in the adjudication process when we need additional information to determine the outcome of the STA. TSA's adjudicators often contact applicants by telephone with questions, and this step typically saves time and expense for the applicant and TSA by resolving issues immediately.

The Privacy Act Notice that operators must provide to applicants when they begin the STA process is set out in the next paragraph. In the Privacy Act Notice, TSA explains why TSA collects personal information from the applicant and how TSA may use the information. We amend the Notice to include an acknowledgement that TSA may notify the applicant's employer if TSA or other law enforcement agency becomes aware that the applicant poses an imminent security threat. TSA does not anticipate that it will be necessary to notify an employer often, but we believe all applicants should be aware that this notification may take place. In addition, we amend the Notice to state that TSA may transmit the applicant's fingerprint information to the DHS' Automated Biometrics Identification System (IDENT) and Social Security Number to the Social Security Administration (SSA). Using IDENT and SSA data are additional tools TSA has available to aid the STA process, and applicants should be aware that we may use those tools in the future. The Privacy Act notice is provided below but may be updated in the future:

> Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113. 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 this information, including your Social Security Number (SSN), will result in delays in processing your application and may prevent completion of your security threat assessment. DHS will use the biographic information to conduct a security threat assessment and where applicable, will forward any fingerprint information to the Federal Bureau of Investigation to conduct a criminal history records check. DHS may also transmit the fingerprint information into the US-VISIT's Automated

> Biometrics Identification System (IDENT). If you provide your SSN, DHS may provide your name and SSN to the Social Security Administration (SSA) in order to compare that information against SSA's records to ensure the validity of your name and SSN. Routine Uses: This information may be shared with third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal, to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication of your applicant or in accordance with the routine uses identified in the Transportation Security Threat Assessment System, DHS/TSA 002.

This rule amends paragraphs (f)-(j) of § 1540.203, which address the comparability of other STAs conducted by TSA or other government agencies. TSA may determine that a threat assessment or background check that TSA conducts for another program, or that another governmental agency conducts, is comparable to the STA outlined in subpart C of part 1540. If an applicant has completed a comparable STA, it will not be necessary for the individual to complete the threat assessment pursuant to part 1540. This process reduces redundant background checks and the costs associated with them. We developed a similar process through notice and comment rulemaking for surface and maritime workers in 49 CFR 1572.5(e), and paragraphs (f)-(j) harmonize with § 1572. Paragraph (i) requires a worker asserting completion of a comparable threat assessment to present the credential that the other agency issued as a result of the assessment, and the operator must retain a copy of it. Also, applicants must notify operators if the agency that issued the credential that corresponds to the comparable assessment revokes the credential for any reason. This is necessary to ensure that a worker who is disqualified from holding access privileges to secure areas in other programs does not continue to have unescorted access to cargo until TSA and the operator can determine if such access is appropriate.

In considering whether another background check is comparable to the STA required in part 1540, TSA examines the standards used for the other threat assessments, such as the kind of databases that the other agency checks and the lookback period for the check. Also, TSA reviews the frequency of the check and the date of the most recent check. If TSA determines that another check is comparable, TSA will notify the public by publishing a notice in the Federal Register, amending rule text through rulemaking in the Federal Register, or posting the information on pertinent websites to ensure that the affected population is aware of the determination.

It is important to note that TSA will consider only threat assessments performed by other government agencies as comparable. 49 CFR 1540.203(f) introductory text. We restrict the checks we will consider as comparable, because critical data sources for security purposes, such as the government's consolidated terrorist watch lists, are not accessible by private entities. This factor is so fundamental to the threat assessments TSA conducts that we are unwilling to accept any other check as comparable. It is also important to note that TSA has the capability to conduct checks perpetually against critical security-related data sources, allowing TSA to compare applicant names automatically with new names that appear on watch lists. This provides a significant improvement over other background checks, and TSA considers it important in making comparability determinations.

Section 1540.203(h) lists the STAs that TSA has determined are comparable to the STA process in part 1540, subpart C. These include a CHRC conducted in accordance with 49 CFR 1542.209, 1544.229, or 1544.230 that also include a TSA name-based check; the STA that TSA conducts under 49 CFR part 1572 for commercial drivers

authorized to transport hazardous materials and maritime workers applying for a Transportation Worker Identification Credential (TWIC); and the STA that CBP conducts for the Free and Secure Trade program.

New § 1540.203(j) provides that the STA expires in five years or when the applicant is no longer in the United States lawfully. If the applicant has completed a comparable threat assessment, the STA will expire five years from the date on which the credential associated with the comparable assessment expires. When the five-year expiration of the STA required in this subpart or a comparable threat assessment approaches, the applicant must submit new identifying information to TSA, and TSA will conduct a new threat assessment.

Section 1540.205-Procedures for Security Threat Assessment

This rule amends § 1540.205 by adding new paragraph (c), which states that if TSA becomes aware that an applicant is the subject of an outstanding want or warrant or is a deportable alien, TSA will notify the appropriate law enforcement or immigration agency.

We added a provision in new paragraph (d)(3) relating to cases in which we believe an applicant may pose an imminent threat. TSA may serve an Initial Determination of Threat Assessment and Immediate Revocation on an applicant if TSA believes the applicant poses an immediate security threat. This situation would most likely involve a worker who completed an STA in the past and has unescorted access to cargo or sensitive areas, if TSA believes it is important to immediately revoke the worker's access even before the worker has an opportunity to file an appeal on the Initial Determination with TSA. TSA developed this process for use in the threat assessments

process for surface and maritime workers, and we believe it is an important tool that should be available in the aviation industry as well.

Section 1540.209-Fees for Security Threat Assessments

Pursuant to sec. 520 of the 2004 DHS Appropriations Act (Pub. L. 108-90, 117 Stat. 1137, Oct. 1, 2003), TSA will charge a fee to individuals who must obtain an STA under this regulation. The fees will reimburse TSA for the costs of administering the program. Pursuant to the general user fee statute (31 U.S.C. 9701) and OMB circular A-25, TSA establishes user fees after providing the public notice and an opportunity to comment on the amount of the fee and the methodology TSA used to develop the fee amount. Therefore, in this preamble, TSA proposes a fee range and invites comment on the amount of the fee and the assumptions we use to estimate the fee. After reviewing all comments received, TSA will issue a Notice in the Federal Register that summarizes and addresses the comments we receive, and establishes the final fee amount, after which the fee will be charged to applicants. Note that the rule text that appears in this IFR relating to fees (49 CFR 1540.209), will not have to be amended at that time because it does not list the specific fee amounts. TSA expects that the total fee will be approximately $13 to $21, although that figure may increase or decrease as the costs involved in the calculation may change between now and when TSA issues the Notice announcing the final fee. TSA will charge a fee once the Notice is published, at which time TSA will announce the exact fee. TSA calculated the estimated fee from an estimate of the number of applicants (population), the cost of processing the applications, the cost of performing the STAs, and the cost of maintaining the information systems to support the process. Table 1

presents the methodology supporting the population estimates. Table 2, in the Costs section, presents the calculations supporting the estimated fee.

Population

TSA estimates that approximately 1,202,566 applicants would be required to complete a STA during the first five years of the program. This estimate is derived from the following population figures that have been gathered for specific segments of the regulated population.

Table 1: CCSP Population Estimates

Operational year	1st Year	2nd Year	3rd Year	4th Year	5th Year	Total
Screening-Base Enrollments	18,200	195,000	328,644	-	-	541,844
Screening-Turnover Enrollments	6,461	75,686	192,355	192,355	192,355	659,212
Approved Validators	1,510	-	-	-	-	1,510
Grand Total	26,171	270,686	520,999	192,355	192,355	1,202,566

Costs

TSA proposes that individuals required to undergo a STA would be required to pay a fee to cover the following costs:

Table 2: CCSP Cost Estimates

Operational Year	1st Year	2nd Year	3rd Year	4th Year	5th Year	Total
Estimated Annual Applicants	26,171	270,686	520,999	192,355	192,355	1,202,566
Cost Components						
Name Check	$102,067	$1,072,055	$2,223,775	$1,237,843	$1,237,843	$5,873,583
Platforms/Systems	$5,584,410	$2,512,723	$2,229,868	$2,293,938	$2,358,006	$14,978,945
Personnel	$1,139,223	$1,370,137	$1,683,908	$1,682,020	$1,754,441	$7,629,729
Grand Totals	$6,825,700	$4,954,915	$6,137,551	$5,213,801	$5,350,290	$28,482,257

For the STA, TSA will check each applicant's information against multiple databases and other information sources. The threat assessment process includes an appeals process for individuals who believe the records upon which TSA bases its determination are incorrect.

TSA would need to implement and maintain the appropriate systems, resources, and personnel to process applicant information and to allow TSA to receive, and act on, the results of the STA.

TSA estimates that the total cost of STA services will be $28,482,257 over five years. The estimate for STA services includes $5,873,583 for TSA name-based checks, $14,978,945 for platforms/systems costs, and $7,629,729 for personnel necessary to facilitate the STA processing.

Total Fee

The fee TSA establishes for the STA should cover all costs related to the STA process. TSA estimates that the resulting applicant charge would be $13 to $21 per applicant, based on the total estimated cost of services provided ($28,482,257). A portion of this total cost will be funded through a $5,875,000 Congressional appropriation. Therefore, the fee will cover only the remaining $22,607,257 in program costs. The remaining cost of $22,607,257 will be divided by the estimated population (1,202,566) receiving the service. The resulting $13 to $21 estimated fee will be sufficient to fully recover the remaining STA costs.

TSA will continue to work to minimize all costs. Additionally, pursuant to the Chief Financial Officers Act of 1990 (Pub. L. 101-576, 104 Stat. 2838, Nov. 15, 1990), DHS/TSA is required to review fees no less than every two years (31 U.S.C. 3512).

Upon review, if TSA finds that the fees are either too high (that is, total fees exceed the total cost to provide the services) or too low (that is, total fees do not cover the total costs to provide the services), TSA will adjust the fee. Finally, TSA will be able to adjust the fees for inflation following publication of the final rule. If TSA were to adjust the fees for this reason, TSA would publish a notice in the Federal Register notifying the public of the change.

TSA invites comment on the proposed fee of $13 to $21 and the methodology and population estimates we used to arrive at this amount.

Revised § 1540.209 provides that TSA will calculate fees for STAs based on widely accepted accounting principles and practices and in accordance with the provisions of 31 U.S.C. 9701 and other Federal law that may affect the collection, computation, or issuance of fees.

Part 1544—Aircraft Operator Security: Air Carriers and Commercial Operators and Part 1546—Foreign Air Carrier Security

Scope

Part 1544 and part 1546 apply to a variety of operators, including different sizes of passenger aircraft and all-cargo aircraft, by U.S. operators and foreign air carriers, respectively. This rule does not apply to all such operators. The requirement to comply with the enhanced cargo screening requirements in the 9/11 Act and this rule apply only to U.S. aircraft operators under § 1544.101(a) and to foreign air carriers under §§ 1546.101(a) and (b). See 49 CFR 1544.205(g) and 1546.205(g). The operators that must comply are air carriers or commercial operators under FAA rule 14 CFR part 119 (which are U.S. operators), and foreign air carriers, in scheduled or public charter

passenger operations with an aircraft having a passenger seating configuration of 61 or more seats, or that will provide deplaned passengers access to a sterile area of an airport or will enplane passengers from a sterile area. See 49 CFR 1540.5, 1544.101(a), and 1546.101(a) and (b). This rule does not apply to general aviation operators.

The 9/11 Act covers cargo originating in the United States as well as cargo destined to the United States from foreign countries. TSA is taking a two-pronged approach to addressing the 100 percent screening mandate for cargo loaded in the United States and cargo loaded outside the United States that is inbound to the U.S. This rule and the CCSP, which require TSA regulatory oversight and enforcement authority for the entire air cargo supply chain, apply only to cargo loaded in the United States. TSA does not have this same regulatory reach to the entire supply chain in the international realm[5] and therefore is taking a different approach to implementing the 9/11 screening mandate for inbound cargo. This approach focuses on harmonization efforts including bi-lateral and multilateral agreements, working on updating International Civil Aviation Organization (ICAO) standards, and applying risk assessment for inbound cargo. Note that U.S. aircraft operators and foreign air carriers that load cargo in other countries inbound to the United States must carry out security measures for that cargo that are set out in their TSA-approved or accepted security programs.

Sections 1544.205 and 1546.205-Acceptance and Screening of Cargo

Section 1544.205 sets forth the requirements for the acceptance and screening of cargo by aircraft operators. Current § 1544.205(e) provides that a full program operator

[5] For example, while TSA regulates both air carriers and indirect air carriers (IACs) domestically, and has regulatory authority over U.S.-bound foreign air carriers, TSA does not have direct authority over foreign IAC equivalents. Through the CCSP, TSA is expanding the domestic screening requirements beyond the aircraft operators and foreign air carriers, to include manufacturers, shippers, IACs, and other entities.

may only accept cargo from a shipper, aircraft operator, foreign air carrier, or indirect air carrier. This rule revises § 1544.205(e) to allow full-program operators to accept screened cargo from a CCSF.

New paragraph (g) includes the major revisions to comply with the 9/11 Act mandates for air cargo screening. TSA adds new paragraph (g)(1) to this section, which provides that, with respect to cargo loaded within the United States, full-program operators must have ensured that at least 50 percent of its cargo was screened prior to transport by February 3, 2009, and that 100 percent will be screened by August 3, 2010.

TSA adds new paragraph (g)(2), which explains the methods of screening identified in the 9/11 Act, including physical examination or non-intrusive methods of assessing cargo such as x-ray systems, explosive detection systems, explosives trace detection, and explosives detection canine teams certified by TSA.

TSA adds new paragraph (g)(3), which imposes requirements for screening methods and identifies who may conduct screening. The following persons may conduct screening: the aircraft operator on an airport; another aircraft operator or foreign air carrier under the Aircraft Operator Standard Security Program or Foreign Air Carrier Model Security Program; or a CCSF.

TSA is harmonizing, to the extent practicable, all requirements for air cargo screening and chain of custody. Aircraft operators now conduct most of their cargo screening on-airport in accordance with their security programs and that will continue. Under section 1544.205(b), aircraft operators must ensure that cargo is screened for any unauthorized explosives as specified in their security programs. If they screen off-airport, however, to promote consistent chain of custody requirements that ensure that the

cargo remains safe and secure from the time of screening until the cargo is transported on a passenger aircraft, new § 1544.205(g)(3) provides that an aircraft operator who screens cargo off-airport must be certified as a CCSF. This ensures that all screening conducted off-airport be subject to the same requirements of part 1549, including the same chain-of-custody requirements

The phrase "on airport" in paragraph (g)(3) has the same meaning as in 49 CFR 1542.205(a)(3). Under that paragraph all areas on-airport that are used for certain cargo functions, including screening, must be a security identification display area (SIDA). A SIDA is that portion of an airport within the United States, specified in the security program, in which individuals must display an airport-issued or approved ID and carry out other security measures. 49 CFR 1540.5 and 1542.205. Personnel screening cargo in such areas are subject to all SIDA requirements including ID media, STAs and CHRCs. TSA has provided guidance regarding what "on-airport" means under § 1542.205(a)(3), and the same guidance applies to § 1544.205(g)(3) in this rule. "On-airport" cargo screening facilities include cargo screening facilities that--

- Are located on the AOA or border the AOA perimeter, as the Airport Security Program (ASP) defines the perimeter's boundary; and
- Share a wall with the AOA perimeter boundary, such that an individual could enter from the public side and exit the facility into the AOA or secured area.

Facilities located entirely outside these areas, including where there is public area between the facility and one of these areas, are "off-airport." The Federal Security Director (FSD) for each airport determines whether a facility is on-airport or off-airport for these purposes.

Under new paragraph (g)(4), if the operator accepts screened cargo from a CCSF, the operator must verify that there has been no break in the chain of custody for the screened cargo between the time of screening and the time the CCSF tenders it to the aircraft operator. If a break has occurred, the aircraft operator must re-screen the cargo prior to transporting it on a passenger aircraft.

In this rule, TSA has amended the text currently located at § 1546.205, which applies to foreign air carriers, to make the text essentially the same as the corresponding provisions in § 1544.205 regarding domestic aircraft operators.

Sections 1544.228, 1546.213, and 1548.15-Access to cargo and cargo screening: Security Threat Assessments for Cargo Personnel in the United States

We amend § 1544.228 to clarify which persons must undergo an STA. Individuals must undergo an STA as specified in the appropriate security programs if they meet any of the following conditions:

- Are authorized by the aircraft operator to have unescorted access to cargo and have knowledge that such cargo will be transported on a passenger aircraft;
- Have unescorted access to cargo that has been screened for transport on a passenger aircraft;
- Perform certain functions related to the transportation, dispatch, or security of cargo for transport on a passenger aircraft or all-cargo aircraft; or
- Screen cargo or supervise the screening of cargo.

Section 1546.213 makes similar clarifications that apply to foreign air carriers. Section 1548.15 makes similar clarifications that apply to IACs. See the discussion of 49 CFR part 1540, subpart C, for a full description of the threat assessment process.

Part 1544 Subpart E and Part 1546 Subpart E–Screener Qualifications

We are removing outdated material in subpart E of parts 1544 and 1546, which apply when the aircraft operator or foreign air carrier conduct screening. TSA added these subparts when the civil aviation security rules were transferred from the FAA to TSA (Civil Aviation Security Rules, 67 FR 8340, Feb. 22, 2002). At that time, TSA included in the rule the screener qualifications and training requirements for aircraft operators and foreign air carriers that were applicable at the time. TSA also included additional requirements for screeners that would apply after November 19, 2002. The rule referred to these as "current screeners" and "new screeners." The new screener requirements became effective several years ago, so we have deleted these outdated sections.

Note that while TSA conducts all screening of passengers and their property in the United States for aircraft operators under a full program under § 1544.101(a), and for foreign air carriers under program under § 1546.101(a) and (b), the aircraft operators and foreign air carriers continue to conduct some passenger and checked baggage screening, such as for certain private charter operations and for certain operations departing locations outside of the United States. They also conduct cargo screening. Thus we continue to have a need for the requirements in subpart E of parts 1544 and 1546.

Part 1549—Certified Cargo Screening Program

Section 1549.1-Applicability

This new part applies to each facility that applies for TSA certification as a CCSF or operates as a CCSF. The regulatory text does not limit who may apply to be certified as a CCSF. Examples of facilities that may apply include: manufacturers; third party

logistics companies; IACs; warehouses, distribution centers and other entities, if they own a facility that directly tenders cargo to an IAC, an aircraft operator, foreign air carrier, or another CCSF for transport on a passenger aircraft. For example, a manufacturer could physically inspect the box prior to closing it and initiating chain of custody, then tender the cargo to a third party logistics company who is a CCSF, who then tenders it to the aircraft operator for transport on a passenger aircraft. If the CCSF could transfer the cargo to a non-regulated entity, it would be difficult to ensure that the chain of custody measures remained intact when the non-regulated entity tendered the cargo to the aircraft operator.

Certifications will apply to a single facility, not to a single company owning several locations where screening would occur, because security measures and the level of security will vary from one facility to another. TSA must evaluate and make a determination on the security measures of the specific facility applying for certification.

Section 1549.3-TSA Inspection Authority

This section codifies TSA's inspection authority. Section 1549.3(a) provides that a CCSF must allow TSA, at any time or place, to enter the facility and make any inspections or tests to determine compliance of the CCSF. These areas may include areas off of the airport or areas operated by the CCSF's agent in furtherance of the CCSF's security responsibilities. Section 1549.3(b) explains that a CCSF must provide evidence of compliance with this part, if TSA requests such evidence.

Section 1549.3(a) states that the CCSF must allow TSA and other authorized DHS officials, at any time and in a reasonable manner, without advance notice, to enter, inspect, and test as necessary to carry out TSA's security-related duties. We note that the

CCSF potentially may operate at all hours of the day. Even when the CCSF is not in operation it must maintain access control measures to, for instance, secure any screened cargo at the facility from entry by an unauthorized person. This section makes clear TSA's authority, and is based on similar sections that apply to airport operators, aircraft operators, and IACs. See 49 CFR 1542.5, 1544.3, 1546.3, and 1548.3. TSA may enter and be present, at any time, areas where a CCSF carries out security measures. TSA inspectors may enter without access media or identification media issued or approved by such a facility, but they will have TSA–issued identification credentials. TSA may copy records, to determine compliance of the facility with applicable regulations, statutory requirements, security programs, directives, or other requirements. Certified cargo screening facilities must allow TSA inspectors to perform these functions, regardless of whether the inspectors provide advance notice of an inspection.

TSA has statutory authorities and responsibilities that support this extensive authority to conduct compliance inspections. For example, TSA must be able to inspect at any time in order to carry out its security-related statutory and regulatory authorities, including the following authorities in 49 U.S.C. 114(f):

(2) Assess threats to transportation.

(7) Enforce security-related regulations and requirements.

(9) Inspect, maintain, and test security facilities, equipment, and systems.

(10) Ensure the adequacy of security measures for the transportation of cargo.

(11) Oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities.

(15) Carry out such other duties, and exercise such other powers, relating to transportation security as the Assistant Secretary considers appropriate, to the extent authorized by law.

Because the transportation system may be compromised by the introduction of an Improvised Explosive Device (IED) or other destructive instrument, the authority for transportation security necessarily includes authority to inspect, as necessary, the facilities that screen cargo prior to aircraft operators' acceptance of that cargo on passenger aircraft. The law does not limit TSA to protecting the security of cargo only while it is on a particular vehicle of transportation, but extends to the entire transportation system. The statute references TSA's responsibility to protect security facilities and transportation facilities.[6] Thus, TSA has explicit authority to inspect all parts of certified cargo screening facilities that relate to screening, including loading and unloading areas, areas where screening and storage occur, and areas where CCSFs prepare or maintain records pertaining to compliance with TSA's requirements. Although TSA has the broad legal authority described above, TSA will conduct inspections in a reasonable manner consistent with TSA guidance for its inspectors.

Section 1549.5-Adoption and Implementation of the Security Program

Section 1549.5 is very similar to § 1548.5 on the Adoption and Implementation of the Security Program for IACs. Section 1549.5(a) specifies that no person may screen cargo to be tendered to 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 carriage on a passenger aircraft, unless that person holds and carries out an approved security program.

[6] 49 U.S.C. 114(f)(9) and 114(f)(11).

Section 1549.5(b) describes the required content of each security program and provides that the security program must be designed to protect against the entry into the aircraft of any unauthorized explosive, incendiary, and other destructive substance or item.

Section 1549.5(c) makes clear that the CCSF is responsible to ensure that their agents and employees carry out the CCSF's security program.

Section 1549.5(d) provides that alternate procedures and amendments to the security program are all part of the CCSF's security program that the CCSF must comply with.

Paragraph (e) is parallel with 49 CFR 1548.5(d), providing basic requirements on the availability of the security program to the firm's personnel and to TSA, and requirements to protect the security program as SSI.

Section 1549.7-Approval, Amendment, Renewal of the Security Program and Certification of a Certified Cargo Screening Facility

To participate as a CCSF, the applicant must apply for a security program and for certification as a CCSF at a particular location in a form and 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 the facility is located in the United States. For example, TSA will not allow a CCSF to be located in Canada and truck cargo to the U.S. for loading onto passenger aircraft. TSA must be able to inspect readily the facility for compliance with TSA requirements.

The applicant must provide information about the business; information about the key individuals at the business (including their names and copies of their identification);

and information required for TSA to conduct STAs of the applicant's employees and senior managers. 49 CFR 1549.7(a)(1).

After the Security Coordinator for an applicant successfully completes an STA, TSA will provide the applicant with the certified cargo screening standard security program. This program is SSI and cannot be shared with unauthorized persons. The applicant may accept the standard program or submit a proposed modification. 49 CFR 1549.7(a)(2)(i). Once the applicant has the security program it can determine how it will meet the requirements of the security program. The applicant must then be assessed by either a TSA-approved validator under 49 CFR part 1522 or by TSA. 49 CFR 1549.7(a)(2)(ii).

Under §§ 1549.7(a)(3), (4), and (5), a CCSF at a particular location may begin screening operations after (1) TSA has reviewed the assessment prepared by the validator and approved and certified the facility, and (2) after the CCSF has successfully completed the training and STAs required under part 1549. Section 1549.7(b) provides that certified cargo screening facilities must apply for a renewal of certification every 36 months, providing the information that TSA requires. Generally, the security program will be a standard program provided by TSA.

Sections 1549.7(c), (d), and (e) include provisions allowing applicants to request amendments to the security program and allowing TSA to amend security programs if warranted by considerations of safety and the public interest. Except in cases of emergency, TSA-initiated amendments will comply with notice and comment procedures before they become effective.

Section 1549.101-Acceptance, Screening, and Transfer of Cargo

This section requires each CCSF to implement procedures in the security program to deter the carriage of explosives or incendiaries onboard aircraft. 49 CFR 1549.101(a). It also requires each CCSF to ensure that cargo is screened and inspected for any unauthorized explosive, incendiary, or other destructive substance or item. 49 CFR 1549.101(b). If the shipper does not consent to search or inspection of the cargo in accordance with this part, the CCSF must not offer such cargo for transport to: (1) another CCSF, (2) an aircraft operator with a full program under 49 CFR 1544.101(a), or (3) a foreign air carrier operating under 1546.101(a) or (b). 49 CFR 1549.101(c).

Finally, § 1549.101(d) requires the CCSF to protect the cargo from unauthorized access from the time the facility screens the cargo until the time the facility tenders it to another CCSF, an IAC, an aircraft operator under part 1544, or a foreign air carrier under part 1546. These chain-of-custody requirements are central to the concept of the CCSP. The regulation does not require specific chain-of-custody controls. Based on knowledge of other programs and on the TSA cargo pilot programs, TSA expects that certified cargo screening facilities will use the following methods: tamper- evident technologies, conveyance level seals, and documented processes. The certified cargo screening standard security program will include specific requirements.

Section 1549.103-Qualifications and Training of Individuals with Security-Related Duties

In accordance with this provision, each CCSF must ensure that employees and agents who are involved in the cargo screening process or who have unescorted access to cargo that has been screened for transport on a passenger aircraft successfully undergo

STAs. 49 CFR 1549.103(a). Each CCSF must also ensure that such individuals have completed the training required by TSA and have knowledge of their responsibilities under the CCSP, the STA provisions of TSA's regulations, and TSA's SSI regulations. 49 CFR 1549.103(b)-(c).

Section 1549.103(d) specifies certain qualifications for individuals performing screening. These qualifications are designed to ensure that these individuals understand the applicable security program, can communicate verbally, and are capable of operating screening equipment.

The requirements in § 1549.103(d) closely parallel the existing requirements for screeners of passengers and checked baggage found in 49 CFR 1544.405, to the extent they apply to the screening of cargo. They include the requirement that the screener be a citizen or national of the United States or be an alien lawfully admitted for permanent residence. The discussion of § 1522.117 in this section-by-section analysis explains the importance of such requirements. A screener must also have a high school diploma or equivalent and must have color perception and physical coordination sufficient to operate effectively cargo screening technologies that a CCSF would use.

Additionally, § 1540.103(d)(4) requires that the screener have 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. This requirement is related to the type of work the screener does. If the screener's duties do not include reading labels, then TSA believes that such an employee need not be able to read and write English sufficiently to write log entries; a supervisor who can read and write English well enough for that purpose would

satisfy that requirement. However, if the employee needs to read shipping documentation or seals on the cargo, English proficiency is required.

Section 1549.105-Recordkeeping

This provision requires each CCSF to maintain records demonstrating compliance with all applicable statutes regulations, directives, orders, and security programs. It also requires the CCSF to maintain copies of training records, documents pertaining to the application and renewal of the facility (including copies of the validator's report), documents establishing TSA's certification and renewal of certification, and records demonstrating satisfaction of the STA requirements. 49 CFR 1549.105(a). With the exception of the training records, the CCSF must retain these records until the next re-certification. 49 CFR 1549.105(b). The facility must retain records indicating satisfaction of the rule's employee training requirements for an individual for 180 days after the individual is no longer employed or acting as an agent of the CCSF. 49 CFR 1549.105(a)(1).

Section 1549.107-Corporate and Facility Security Coordinators

This section requires each facility to designate a Security Coordinator and alternate appointed at the corporate level, and a Security Coordinator and alternate appointed at each facility that will conduct screening. A corporate level Security Coordinator is needed if a single company has multiple facilities. The Security Coordinator must have corporate authority to represent and speak for the company and to serve as TSA's point of contact with that company. A facility-based Security Coordinator is needed so that TSA has a point of contact that is familiar with the operations and procedures of the particular facility certified as a CCSF. A corporate level

Security Coordinator may also serve as a facility level Security Coordinator. Both Security Coordinators, or their alternates at the corporate and facility level, must be available 24-hours per day to address any adverse security incidents that may arise or to receive information from TSA or others that might jeopardize the security of the cargo handled at the facility.

Section 1549.109-Security Directives and Information Circulars

This provision requires each CCSF to comply with any security directives that TSA may issue to address a security concern that requires immediate action. TSA may issue Information Circulars, which provide information to regulated parties. These do not include mandatory security measures but provide useful information about potential threats.

Section 1549.111-Security Threat Assessments for Personnel of Certified Cargo Screening Facilities

This section requires personnel of certified cargo screening facilities to undergo the STA described in 49 CFR part 1540, subpart C. We are requiring STAs for the following individuals:

- Individuals authorized to perform cargo screening or supervise cargo screening;
- Individuals authorized to have unescorted access to cargo from the time of screening until the time it is offered to an IAC for transport on passenger aircraft, an aircraft operator under part 1544, or a foreign air carrier under part 1546;
- The senior manager or representative of the CCSFs in control of the operations; and
- Security Coordinators and their alternates.

TSA is requiring STAs for the individuals listed above to reduce the likelihood of a terrorist's gaining employment in a position with access to cargo for the purpose of introducing an explosive or other destructive substance into cargo on a passenger aircraft. Extending the STAs to such individuals in a CCSF provides a degree of security comparable to TSA's other programs, including the IAC program, in that all personnel of regulated parties with access to cargo from the time of screening until the time the aircraft operator loads it will undergo a check against the terrorist databases. For a full description of the STA process, see the discussion of 49 CFR part 1540, subpart C.

VI. Good Cause for Immediate Adoption

TSA is taking this action without providing the public prior opportunity for notice and comment. The 9/11 Act requires TSA to have developed a system for the screening of 50 percent of cargo transported by passenger aircraft by February 2009, and to develop a system for the screening of 100 percent of such cargo by August 2010. In 49 U.S.C. 44901 (g)(2)(A), Congress specifically authorized TSA to issue an IFR "as a temporary regulation to implement this section without regard to the provisions of chapter 5 of title 5." The Act further states that if TSA issues an IFR, then TSA must follow it with a final rule within 12 months of the effective date of the IFR. 49 U.S.C. 44901(g)(2)(B)(i).

TSA cannot meet the screening requirements established in the 9/11 Act for cargo loaded in the U. S. without a system in place to screen cargo off-airport by parties other than aircraft operators, as this rule will accomplish. TSA could not achieve this mandate by relying solely on aircraft operators and foreign air carriers to conduct screening. There is insufficient space and capacity for aircraft operators and foreign air carriers to screen the approximately 12 million pounds of cargo transported on passenger aircraft in

the United States. Much of this cargo is gathered by IACs off-airport, consolidated into Unit Load Devises or pallets, and brought to the airport for loading on aircraft. There currently is not a way to adequately screen most consolidations of cargo without breaking them down. Aircraft operators and foreign air carriers do not have sufficient space or time to remove the cargo from the consolidations, screen it, and re-consolidate it, before loading it onto aircraft. This rule establishes more cost-effective and efficient options for CCSFs to screen the cargo off-airport before it is consolidated so that it may be taken to the airport and loaded onto aircraft with little delay. Aircraft operators, foreign air carriers, IACs, and facilities that may decide to become CCSFs must have sufficient finality in the regulations to develop their screening programs and have them fully operational in time to meet the statutory deadlines.

It would be contrary to the public interest to delay this rule. Meeting the statutory requirements for the screening of cargo on passenger aircraft with this IFR will provide substantial security benefits by providing the stakeholders with finality in the rule at an earlier stage, which will allow them to determine how best to comply with the requirements. For instance, IACs, shippers, and other facilities that choose to become CCSFs will have time to comply with the new requirements and become certified. The rationale for issuing this rule as an IFR is fully consistent with sections 553(b) and (d) of the Administrative Procedure Act (APA) (5 U.S.C. 553), which authorize agencies to issue final rules without affording the public a prior opportunity to comment is "impracticable, unnecessary, or contrary to the public interest."

VII. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 et seq.) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. This interim final rule contains new information collection activities subject to the PRA. Accordingly, TSA has submitted the following information requirements to OMB for its review.

Title: Certified Cargo Screening Program Interim Final Rule.

Summary: Section 1602 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53) (August 2007) requires the development of a system to screen 100 percent of the cargo transported on a passenger aircraft operating within the United States by August 2010 and to have screened 50 percent of all air cargo by February 2009. This rule amends several parts of Title 49 of the Code of Federal Regulations (CFR) and adds new parts, as described in prior sections of this preamble. The rule creates several new information collections.

Through this rule, TSA is including the following information collections:

First, an entity that seeks to become a CCSF under 49 CFR part 1549 must submit an application to TSA.

Second, a validator from a TSA-approved validation firm must assess each CCSF every three years. An entity that seeks to become a TSA-approved validation firm under 49 CFR part 1522 must submit an application to TSA.

Third, TSA must conduct STAs for key personnel of CCSFs and validation firms. The key personnel must submit personal data to TSA for the STAs. This STA portion is a previously approved collection under OMB control number 1652-0040, but this IFR expands the population from which the information is collected.

Fourth, CCSFs and TSA-approved validation firms must accept or submit security programs for approval. CCSFs must accept a standard security program provided by TSA or submit a proposed modified security program to the designated TSA official for approval initially and periodically thereafter as required. Validation firms must accept a standard security program provided by TSA or submit a proposed modified security program to the designated TSA official for approval initially and periodically thereafter as required. The validation firm must also submit a supplement to the security plan 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.

Fifth, CCSP participants, indirect air carriers, and TSA-approved validation firms must maintain records of compliance with the IFR and make them available for TSA inspection (see 49 CFR 1522.129 and 1549.105).

Sixth, TSA-approved validation firms must submit their validators' assessments of CCSFs to TSA.

Finally, CCSFs and air carriers must submit TSA-determined monthly cargo screening metrics to TSA.

Use of: TSA will use the applications of entities seeking to become CCSFs to approve the entity as a CCSF. TSA will use the applications of entities seeking to

become TSA-approved validation firms to approve the entities as approved validation firms. TSA will collect personally identifiable information from CCSFs, validation firms, and indirect air carriers about their key personnel in order to conduct STAs on these individuals, which is an important security measure that should apply to individuals who screen cargo and have unescorted access to screened cargo as well as to other key individuals. CCSF and validation firm security programs are necessary because they contain specific measures to deter incidents that may jeopardize transportation security. CCSFs must maintain records and provide TSA-approved validators access to their records, equipment, and facilities necessary for the validators to conduct assessments. TSA will require the validators to submit their assessment reports to TSA in a manner and form prescribed by TSA, and to also retain validation reports that they have prepared for a minimum of 36 months. TSA will use the reports to determine whether CCSFs and validation firms are complying with TSA regulations. Finally, CCSFs and TSA-approved validation firms must submit security programs for approval. These security programs contain specific measures to deter incidents that may jeopardize transportation security. TSA requires CCSFs to provide information on the amount of cargo screened at an approved facility in order to evaluate the compliance and performance of the CCSFs and to provide information needed for congressional reporting and future rulemaking relating to air cargo security.

Respondents (including number of): The likely respondents to this proposed information requirement are the 22,541 entities that seek to become CCSFs under 49 CFR part 1549 and the 83 entities that seek to become TSA-approved validation firms.

Frequency: CCSFs will submit an application for recertification every three years. The rule will require CCSFs to submit an application once annually. TSA estimates that CCSFs, TSA-approved validation firms, and indirect air carriers will submit personally identifiable information of their key personnel so that TSA can conduct STAs every five years. The rule will require CCSFs and validation firms to accept or submit a security program once, and TSA estimates CCSFs will submit updates to their security program on average once annually. TSA estimates that validators will submit their assessment reports to TSA as frequently as they perform the assessments. The recordkeeping requirements will be continuous. The requirement for CCSFs to provide information on the amount of cargo screened and other screening data at an approved facility will be a monthly collection.

Annual Burden Estimate: TSA estimates that the 7,514 entities who will seek to become CCSFs annually will spend approximately 2 hours each to complete the applications for an annual burden of 15,028 hours. TSA estimates that the 28 entities who will seek to become TSA-approved validation firms annually will spend approximately 30 minutes each to complete the applications for an annual burden of 14 hours. TSA estimates 312,433 annual responses from CCSFs, validation firms, and indirect air carriers and the time spent annually submitting personally identifiable information of key personnel for TSA to conduct STAs for an annual burden of 78,108 hours. The time to complete an STA application is estimated at 15 minutes per individual. TSA has estimated that a total of 16,989 CCSFs and validation firms will adopt their security programs for an average of 5,663 security programs annually. Each firm will devote approximately 42 hours to their initial security program, resulting in an

annual burden of 237,846 hours. TSA has estimated that a total 31,589 CCSFs and validation firms will be required to maintain and update their security programs for an average of 10,530 security programs updated annually. Each firm will devote approximately 4 hours each annually, beginning in the second year, updating their security programs for an annual hour burden of 42,119. TSA estimates all CCSFs and validation firms will be required to maintain records of compliance with the IFR. This includes a time burden of approximately 5 minutes (0.083 hours) for every CCSF and validation firm employee who is required to have an STA as well as other records of compliance. This also includes validation firm filings of validation assessment reports, resulting in 312,433 annual record updates. TSA estimates an annual burden of approximately 25,932 hours. TSA estimates that 28 TSA-approved validation firms will spend approximately 4 hours each annually to prepare their findings and submit them to TSA, for annual burden of 22,541 hours. TSA estimates that 5,635 CCSFs will complete monthly cargo reports at an estimated time of one hour per week for an estimated annual burden of 293,037 hours.

Information Collection and Hour Burden Summary (17,117 Unique Respondents Over 3 Years)						
Function	Annual Respondents	Annual Responses	Time Per Response	Annual Hours (3-Year Total)	TSA Form Number	Regulation Cite
CCSF Applications	(Initial application is a one time collection, re-certification is every three years)					
One Year	7,514	7,514	2 hours	15,028	419E	§ 1549.7
Three Years	22,541	22,541	2 hours	45,083	419E	§ 1549.7
Validation Firm Applications	Annual collection					
One Year	28	28	.5 hours	14	419G	§ 1522.107
Three Years	83	83	.5 hours	42	419G	§ 1522.107
STA Applications	Collected every five years after initial application					
One Year	312,433	312,433	.25 hours	78,108	419F	§§ 1549.11 & 1549.103
Three Years	937,300	937,300	.25 hours	234,325	419F	§§ 1522.117& 1522.121
Security Programs						
Creations	One time collection					
One Year	5,663	5,663	42 hours	237,846		§ 1522.105
Three Years	16,989	16,989	42 hours	713,538		§ 1522.105
Updates	Once annually					
One Year	10,530	10,530	4 hours	42,119	N/A	§ 1549.5
Three Years	31,589	31,589	4 hours	126,356		§ 1549.5
Recordkeeping	Continuous as needed					
One Year	312,433	312,433	.083 hours	25,932	N/A	§§ 1549.105 & 1522.129
Three Years	937,300	937,300	.083 hours	77,796		§§ 1549.105 & 1522.129
Validation Assessment Reports	Continuous as needed					
One Year	28	5,635	4 hours	22,541	N/A	§ 1522.127
Three Years	83	16,906	4 hours	67,624		§ 1522.127
Cargo Reporting	Monthly collection					
One Year	5,635	67,624	52 hours	293,037	N/A	§ 1549.105
Three Years	16,906	202,872	52 hours	879,112		§ 1549.105
CCSF Subset- 1 year	121	1,452	2.5 hours	3,630	N/A	§ 1549.105
TOTAL for One Year	**654,385**	**723,312**		**718,255**		
TOTAL for Three Years	**1,962,791**	**2,165,580**		**2,143,875**		

TSA requests comments to--

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Individuals and organizations may submit comments on the information collection requirements by [Insert date 60 days after publication in the Federal Register]. Direct the comments to the address listed in the ADDRESSES section of this document, and fax a copy of them to the Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: DHS-TSA Desk Officer, at (202) 395-5806. A comment to OMB is most effective if OMB receives it within 30 days of publication.

As protection provided by the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

VIII. Economic Impact Analyses

A. Regulatory Evaluation Summary

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866 (EO 12866), Regulatory Planning and Review, directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 et seq., as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. 2531-2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

TSA has prepared a separate detailed analysis document which is available to the public in the docket. With respect to these analyses, TSA provides the following conclusions and summary information:

- This rule is considered to be an economically significant rule within the definition of EO 12866, as estimated annual costs or benefits exceed $100 million in any year. TSA has included the mandatory OMB Circular A-4 Accounting Statement in the separate analysis document and thus has not repeated it here.

- Under the Regulatory Flexibility Act of 1980, an agency need not publish a formal analysis of the impact to small entities with the interim final rule. Therefore, TSA has not determined whether or not this interim final rule will have a significant impact on a substantial number of small entities.
- This regulatory evaluation provides the required assessment of the Trade Agreement Act of 1979.
- The regulatory evaluation provides the required written assessment of Unfunded Mandates. This interim final rule is not likely to result in the expenditure by State, local, or tribal governments, in the aggregate, of $100 million or more annually (adjusted for inflation). However, because the rule is economically significant as defined by Executive Order 12866, it does have an unfunded mandate impact on the economy as a whole. The separate analysis of the costs and benefits of the rule satisfies the requirements of the Unfunded Mandates Reform Act.

B. Executive Order 12866 Assessment

This IFR is a major rule within the definition of Executive Order (EO) 12866, as annual costs or benefits to all parties exceed the $100 million threshold in any year. TSA has not identified any significant economic impacts for each of the required analyses of small business impact, international trade, or unfunded mandates. This summary highlights the costs and benefits of the rule.

Costs

This section summarizes the types of costs of this rule, which would be borne by five relevant parties: CCSFs, non-CCSF entities that receive screened cargo from CCSFs,

validation firms, aircraft operators (including, in this context, both U.S. aircraft operators and foreign air carriers), and TSA. A summary table at the end of this section provides an overview of the cost estimates. The following paragraphs provide brief descriptions of the cost components. This rule will require expenditures by CCSFs, approved validation firms, and aircraft operators. CCSFs and approved validation firms must adopt security programs and, in the case of CCSFs, undergo assessment of their security measures by a TSA-approved validation firm prior to joining the program. CCSFs and validation firms must complete TSA-conducted STAs for individuals who will be screening cargo or who have unescorted access to screened cargo, as well as for personnel supporting these functions. CCSFs and validation firms must employ security coordinators and alternates.

CCSFs must also implement training for individuals who perform security-related duties. CCSFs may need to purchase equipment to perform their responsibilities under this program. Validation firms will need to pay for training for individuals involved in conducting assessments. Aircraft operators will need to purchase equipment and hire personnel to handle their additional screening burdens.

TSA will incur costs to implement the rule. These will include the costs associated with reviewing applications and security programs, reviewing validation reports, conducting STAs, and inspecting CCSFs and validation firms. In addition, TSA will incur the cost of developing or approving training programs for validation firms and TSA employees and of developing the Air Cargo Data Management System. Total TSA costs can be found in the Total section in Table 1, and in Table 32 of the Regulatory Evaluation.

Total

In summary, over the 10-year period of the analysis, TSA estimates the aggregate costs of this rulemaking to total approximately $2.8 billion, undiscounted. Discounted at seven percent, the cost is $1.9 billion, and discounted at three percent, the cost is $2.4 billion. Additionally, industry will bear a cost for delayed shipment of cargo estimated at $297.1 million over the 10-year analysis period ($203.1 million discounted at seven percent and $250.4 million discounted at three percent). The regulatory impact analysis provides detailed estimates of these costs.

TSA anticipates bearing costs to administer the provisions of the rulemaking at $384 million over the 10-year analysis period.

TSA presents details in the regulatory impact analysis on how it developed these estimates. The following table displays the annual costs of the rule over the 10-year analysis period. The total is broken out by costs to TSA; costs to industry, estimated using the U.K. Known Consignor program as a proxy for screening fees; and the estimated delay costs due to screening. The TSA total represents the estimated costs TSA will incur to implement the CCSP and enforce compliance. The industry cost is estimated using the U.K. fee proxies and accounts for the 70 percent of cargo shipped on passenger planes expected to be screened at CCSFs as well as the additional fifteen percent that aircraft operators are expected to screen. The delay cost assumes the 30 percent of cargo expected to be screened by the aircraft operators will be the only cargo subject to delay.

Table 1: 10-Year Total Cost Summary of CCSP ($millions)

Year	TSA Cost	Industry Cost	Delay Cost	Total Cost	Discounted (3 percent)	Discounted (7 percent)
1	$62.1	$171.3	$23.6	$257.0	$249.5	$240.2
2	$24.5	$179.9	$24.8	$229.3	$216.1	$200.2
3	$25.7	$188.9	$26.0	$240.7	$220.3	$196.5
4	$35.4	$198.4	$27.3	$261.1	$232.0	$199.2
5	$28.7	$208.3	$28.7	$265.6	$229.1	$189.4
6	$38.8	$218.7	$30.1	$287.7	$240.9	$191.7
7	$43.5	$229.6	$31.7	$304.8	$247.8	$189.8
8	$37.1	$241.1	$33.2	$311.4	$245.8	$181.2
9	$38.9	$253.2	$34.9	$326.9	$250.6	$177.8
10	$49.4	$265.8	$36.6	$351.8	$261.8	$178.9
Total	**$384.2**	**$2,155.1**	**$297.1**	**$2,836.4**	**$2,394.0**	**$1,945.0**
Low	$262.4	$1,795.9	$281.5	$2,339.9	$1,974.7	$1,604.0
High	$512.8	$2,514.3	$318.9	$3,346.0	$2,824.3	$2,294.8

100 Percent Aircraft Operator Screening

As an alternative to establishing the CCSP, TSA considered meeting the statutory requirements by having aircraft operators screen cargo intended for transportation on passenger aircraft—that is, continuing the current cargo screening program but expanding it to 85 percent of air cargo on passenger aircraft. TSA estimates that the remaining fifteen percent will be transferred to alternate means of transportation due to the increased delays and costs of shipping this IFR might incur. The cost of the modal shift assumed by TSA was not estimated as the cost components of this shift would be difficult to estimate. Under this alternative, aircraft operators would bear the costs of screening additional cargo, and industry would bear significant costs because of delays. TSA would not incur costs as a result of this alternative. TSA currently requires aircraft operators to screen cargo intended for transport on passenger aircraft at levels set out in their security programs. As a result, TSA would not have to take any new action.

Under this alternative, the cost drivers for this alternative are screening equipment, personnel for screening, training of personnel, and delays. Delays are the largest cost component, totaling $7.0 billion over 10 years, undiscounted. In summary, the undiscounted 10 year cost of the alternative is $11.1 billion dollars. Discounted at three percent, the cost is $9.4 billion and discounted at seven percent, the cost is $7.7 billion. The following table presents the costs of the 100 percent aircraft operator screening alternative, as well as high and low variations and totals discounted at 3 percent and 7 percent.

Table 2: 10-Year Total Cost Summary of 100 Percent Air Carrier Screening ($millions)

Year	Equipment	Personnel	Training	Domestic Delays	Total	3% Discount	7% Discount
1	$85	$307	$4.9	$613	$1,009	$980	$943
2	$10	$322	$2.7	$631	$965	$910	$843
3	$10	$338	$2.9	$649	$1,000	$915	$816
4	$10	$355	$3.0	$668	$1,035	$920	$790
5	$10	$373	$3.2	$687	$1,073	$925	$765
6	$10	$391	$3.3	$707	$1,112	$931	$741
7	$10	$411	$3.5	$728	$1,152	$937	$718
8	$85	$431	$3.7	$750	$1,269	$1,002	$739
9	$10	$453	$3.8	$772	$1,239	$950	$674
10	$10	$476	$4.0	$796	$1,286	$957	$654
Total	$249	$3,856	$35.0	$7,002	$11,142	$9,427	$7,683
Low	$187	$2,892	$26	$5,251	$8,356	$7,070	$5,762
High	$311	$4,820	$44	$8,752	$13,927	$11,784	$9,603

Benefits

The interim final rule will allow for more standard governance in cargo screening and will provide benefits in terms of increased security of commercial passenger aviation. The benefits are four fold. First, the passenger airline industry will be more firmly protected against an act of terrorism or other malicious behaviors by the screening of 100 percent of cargo shipped on passenger aircraft; currently, only a portion of this cargo is screened before being loaded onto the plane. Second, allowing the screening process

to occur throughout the supply chain via the CCSP will reduce potential bottlenecks and delays at the aircraft operators. Third, the interim final rule will allow the market forces to identify the most efficient venue for screening along the supply chain. As the most cost-effective venue for screening varies widely depending on the type of goods being shipped on passenger aircraft operators, the interim final rule will permit any entity on the supply chain to apply for TSA certification to screen cargo and apply chain-of-custody procedures to secure that cargo. Finally, validation firms will perform assessments of the entities that become CCSFs. These assessments will enable TSA to set priorities for compliance inspections while leveraging TSA inspectors with vetted and trained validation firms, thereby adding an extra layer of security.

Alternatively, TSA has assessed the benefits of this rule via a break-even analysis of the cost of the reduction in risk with the dollar amount of the benefit from the rule. The break-even analysis illustrates the tradeoff between program costs and program benefits. For purposes of the analysis, TSA evaluated four scenarios in which an explosive device was placed in the aircraft's cargo hold via air cargo and detonated, destroying the airplane and all passengers and crew on board. For each scenario, TSA derived a total monetary cost of consequence from an estimated value of the statistical human lives lost and the value of the plane (including cargo) destroyed. TSA obtained a value of the monetary cost of an attack under a certain probability (the value of which equals the total estimated monetary cost of the attack multiplied by the probability of an attack of that nature over a year-long time period) and compared it to the undiscounted, annualized cost of the CCSP to estimate how often an attack of that nature would need to be averted for the expected benefits to equal costs.

Table 3 summarizes the results of the break-even analysis, based on the 10-year cost of the rule, annualized at seven percent. Below we describe the four scenarios that we used in that analysis. To judge the value or effectiveness of this IFR in the context of these scenarios, it is necessary to compare the extent of monetary consequence from a successful attack with the cost of a program like the IFR that would be deployed to reduce the risk or likelihood of such an attack being successfully undertaken.

The first scenario describes the impact of a situation in which an explosive device placed in the cargo shipped on the flight in the belly of the plane destroys a standard narrow body aircraft (from the fleets used by major U.S. aircraft operators) during flight. This incident results in the loss of the lives of all passengers and crew members on board, along with the total destruction of the airplane. TSA estimated 119 total people to be on board, including both passengers and crew. The value of these statistical lives is approximately $690.2 million in 2006 U.S. dollars, based on the Department of Transportation Value of a Statistical Life (VSL) estimation of $5.8 million per person. The estimated aircraft cost is just under $17 million on average, again in 2006 dollars. Adding these two together, and assuming no damage on impact to the crash site, TSA estimates the total monetary consequence of the attack at $707.2 million.

The second scenario depicts a situation where an explosive device placed in the cargo shipped on the flight in the belly of the plane destroys an average U.S. commercial passenger aircraft (from the fleets used by major US aircraft operators) in flight. This attack results in loss of life for passengers and crew members, along with complete destruction of the aircraft. Based on data reported in the FAA Critical Values Guidance, there is an assumed loss of 133 lives (128 passengers and 5 crew members), along with

an assumed complete loss of the aircraft, which on average would be valued at $22 million in 2006 dollars. The monetary estimate associated with the loss of life is $771 million. Combining the loss of life monetary estimate with the weighted average aircraft market value, TSA estimates the total monetary consequence of this scenario at $793 million.

The third scenario depicts a situation where an explosive device placed in the cargo shipped on the flight in the belly of the plane destroys an average U.S. commercial passenger wide-body aircraft (from the fleets used by major U.S. aircraft operators) in flight. This attack scenario, like the first scenario, results in loss of life for passengers and crew members, along with complete destruction of the wide-body aircraft. Based on data reported in the FAA Critical Values Guidance, there is an assumed loss of 210 lives (202 passengers and 8 crew members) along with the complete loss of the aircraft, which on average would be valued at $49.6 million in 2006 dollars. Using the DOT VSL of $5.8 million, the monetary estimate associated with the loss of life is $1.22 billion. Combining the loss of life monetary estimate with the weighted average aircraft market value, TSA estimates the total monetary consequence of this scenario at $1.27 billion.

The fourth scenario is an extension of the third that takes into account a situation involving multiple planes destroyed by an explosive device. In our case, four wide body aircraft are the targets of the attack. Our estimation of the monetary damage took the value of the single wide body aircraft attack and multiplied that total monetary consequential amount by a factor of four. Therefore, the resulting estimate of monetary damage caused in this scenario is $5.1 billion, in 2006 dollars. This includes

approximately 840 passenger and crew member lives lost, and an estimated $198.2 million loss due to the destruction of the four wide body airplanes.

The table below presents the number of attacks averted (expressed as a number of years between attacks), required for the IFR to break even under each of the four scenarios. In this analysis the comparison is made between the estimated scenario consequence and the seven percent discount annualized Air Cargo Screening IFR cost of $276.9 million; the "required risk reduction in attack frequency" for break-even can be derived as the multiplicative inverse of the ratio between this annualized program cost and the scenario consequence total (a ratio which expresses a breakeven annual likelihood of attack). As shown in the following table, the rule will need to reduce the existing or baseline frequency of terror attack by one attack every 2.6 years for Scenario 1, one attack every 2.8 years for Scenario 2, one attack every 4.5 years for Scenario 3, or one attack every 18.2 years for Scenario 4 in order for the IFR to break even.

Table 3: Frequency of Attacks Averted for Passenger Air Cargo Screening IFR Costs to Equal Expected Benefits, by Attack Scenario (Annualized at 7 Percent)

	Attack Scenario	Lives Lost	Valuation at $0.0058 M ($ billion)	Avg. Aircraft Market Value ($ billion)	Property Loss ($ billion)	Total Consequence ($ billion)	Attacks Averted by Air Cargo Sec to Break-Even
		A	B = A x 0.0058	C	D	E = B + C + D	= E ÷ $276.9**
1	Narrow Body Target	119	$0.69	$0.017	$0.0	$0.71	One every 2.6 years
2	Avg. AO Target	133	$0.77	$0.022	$0.0	$0.79	One every 2.8 years
3	Wide Body Target	210	$1.22	$0.050	$0.0	$1.27	One every 4.5 years
4	Multiple Wide Body	840	$4.87	$0.198	$0.0	$5.07	One every 18.2 years

**The total cost of the rule annualized at 7 percent.

C. Regulatory Flexibility Act Assessment

Sections 603(a) and 604(a) of the Regulatory Flexibility Act (RFA) require that, when an agency issues a interim final rule or promulgates a final rule "after being required . . . to publish a general notice of proposed rulemaking," the agency must determine whether a proposed or final rule will have a significant economic impact on a substantial number of small entities and, if so, must prepare a regulatory flexibility analysis as described in the Act. For purposes of the RFA, small entities include small businesses, not-for-profit organizations, and small governmental jurisdictions. Individuals and States are not included in the definition of a small entity. These requirements do not apply where, as here, an agency issues an interim final rule. Congress explicitly authorized TSA to issue an IFR in the 9/11 Act. TSA invites comments that address whether this rule would have a significant economic impact on a substantial number of small entities. TSA will consider this information in developing the final rule.

D. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this interim final rule and has determined that the same measures must apply to both U.S. aircraft operators and foreign air carriers loading

cargo on passenger aircraft. At most, the impact of this rule creates an even competitive cost structure.

E. Unfunded Mandates Assessment

The Unfunded Mandates Reform Act of 1995 (UMRA) is intended, among other things, to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of UMRA requires each Federal agency to prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may result in an expenditure of $100 million or more (adjusted annually for inflation) in any one year by State, local, and tribal governments, in the aggregate, or by the private sector, such a mandate is deemed to be a "significant regulatory action." This interim final rule does not exceed this threshold with respect to State, local, and tribal governments, because it does not require them to take any action. The impact on the overall economy, however, does exceed the threshold, resulting in an unfunded mandate on the private sector; this regulatory evaluation documents the costs and alternatives associated with this regulatory action. TSA will publish a final analysis, including its response to public comments, when it publishes a final rule.

IX. Executive Order 13132, Federalism

TSA has analyzed this final rule under the principles and criteria of Executive Order 13132, Federalism. We determined that this action will not have a substantial direct effect on the States, or the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government, and, therefore, does not have federalism implications.

X. Environmental Analysis

We have analyzed this interim final rule under DHS Management Directive 5100.1 "Environmental Planning Program" (see also 71 FR 16790, Apr. 4, 2006), which guides DHS in complying with the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321-4370f). We have concluded that this rule is part of a category of actions described in items A3, A4, A7, B3, H1 and H2 of Table 1 in Appendix A of the Management Directive. This interim final rule would not have individually or cumulatively a significant effect on the human environment and, therefore, neither an environmental assessment nor an environmental impact statement is necessary.

XI. Energy Impact Analysis

TSA has assessed the energy impact of this rule in accordance with the Energy Policy and Conservation Act (EPCA), Pub. L. 94-163, as amended (42 U.S.C. 6362). We have determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects

49 CFR Part 1515

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

49 CFR Part 1520

Air transportation, Law enforcement officers, Maritime carriers, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1522

Accounting, Aircraft operators, Aviation safety, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1540

Air carriers, Aircraft, Airports, Civil aviation security, Law enforcement officers, Reporting and recordkeeping requirements, Security measures, Screening.

49 CFR Part 1542

Air carriers, Aircraft, Airport security, Aviation safety, Security measures.

49 CFR Part 1544

Air carriers, Aircraft, Aviation safety, Freight forwarders, Incorporation by reference, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1546

Aircraft, Aviation safety, foreign air carriers, Incorporation by reference, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1549

Air transportation, Reporting and recordkeeping requirements, Security measures.

The Amendments

For the reasons set forth in the preamble, the Transportation Security Administration amends Chapter XII, of Title 49, Code of Federal Regulations as follows:

SUBCHAPTER A--ADMINISTRATIVE AND PROCEDURAL RULES

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

1. The authority citation for part 1515 continues to read as follows:

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.

2. Amend § 1515.1 by revising paragraph (a) to read 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.

* * * * *

3. Amend § 1515.9 by adding paragraphs (a)(3), (c)(1)(iv) and (v), and revising paragraph (f)(3) to read 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.

4. Amend § 1515.11 by revising paragraph (a)(3) to read 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

5. The authority citation for part 1520 continues to read as follows:

Authority: 46 U.S.C. 70102-70106, 70117; 49 U.S.C. 114, 40113, 44901-44907, 44913-44914, 44916-44918, 44935-44936, 44942, 46105.

§ 1520.3 [Amended]

6. In § 1520.3, remove the definition of "Security program".

7. Amend § 1520.5 by revising paragraph (b)(1) to read 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.

* * * * *

8. Amend § 1520.7 by revising paragraph (b) to read 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.

* * * * *

9. Add new part 1522 to Subchapter B to read as follows:

PART 1522—TSA-APPROVED VALIDATION FIRMS AND VALIDATORS

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.

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 AUTHORITY: GENERAL RULES

10. The authority citation for part 1540 continues to read as follows:

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

Subpart A--General

11. Amend § 1540.5 to by adding definitions of "certified cargo screening program", ''certified cargo screening facility", and "standard security program" in alphabetical order to read 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.

* * * * *

12. Revise part 1540, subpart C to read as follows:

Subpart C—Security Threat Assessments

Sec.

§ 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.

13. Add new subpart D to part 1540 to read as follows:

Subpart D--Responsibilities of Holders of TSA-Approved Security Programs

Sec.

Subpart D--Responsibilities of Holders of TSA-Approved Security Programs

§ 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 1544—AIRCRAFT OPERATOR SECURITY: AIR CARRIERS AND COMMERCIAL OPERATORS

14. The authority citation for part 1544 continues to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44913–44914, 44916–44918, 44932, 44935–44936, 44942, 46105.

Subpart C—Operations

15. Amend § 1544.205 by revising paragraph (e) and adding new paragraph (g) to read 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.

16. Revise § 1544.228 to read 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.

Subpart E—Screener Qualifications When the Aircraft Operator Performs Screening

17. Revise § 1544.401 to read 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 [Removed and Reserved]

18. Remove and reserve § 1544.403.

§ 1544.405 Qualifications of screening personnel.

19. Revise the heading of § 1544.405 to read as set forth above.

20. Amend § 1544.407 by revising the heading and paragraph (c) to read 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 Integrity of screener tests.

21. Revise the heading of § 1544.409 to read as set forth above.

§ 1544.411 Continuing qualifications of screening personnel.

22. Revise the heading of § 1544.411 to read as set forth above.

PART 1546—FOREIGN AIR CARRIER SECURITY

23. The authority citation for part 1546 continues to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44914, 44916–44917, 44935–44936, 44942, 46105.

Subpart C—Operations

24. Amend § 1546.205 by revising paragraphs (d) and (e) and adding new paragraph (g) to read 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.

25. Revise § 1546.213 to read 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.

Subpart E—Screener Qualifications When the Foreign Air Carrier Conducts Screening

26. Revise § 1546.401 to read 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 [Removed and Reserved]

27. Remove and reserve § 1546.403.

§ 1546.405 Qualifications of screening personnel.

28. Revise the heading of § 1546.405 to read as set forth above.

§ 1546.407 Training, testing, and knowledge of individuals who perform screening functions.

29. Revise the heading of § 1546.407 to read as set forth above.

§ 1546.409 Integrity of screener tests.

30. Revise the heading of § 1546.409 to read as set forth above.

§ 1546.411 Continuing qualifications of screening personnel.

31. Revise the heading of § 1546.411 to read as set forth above.

PART 1548—INDIRECT AIR CARRIER SECURITY

32. The authority citation for part 1548 continues to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901-44905, 44913-44914, 44916-17, 44932, 44935-44936, 46105.

33. Revise § 1548.7(f) to read 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.

* * * * *

34. Revise § 1548.15 to read 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.

35. Revise § 1548.16(a) to read 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.

* * * * *

36. Add new § 1548.21 to read as follows:

§ 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.

37. Add new part 1549 to subchapter C to read as follows:

PART 1549—CERTIFIED CARGO SCREENING PROGRAM

Subpart A--General

Sec.

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44913–44914, 44916–44917, 44932, 44935–44936, 46105.

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.

Issued in Arlington, Virginia, on September 1, 2009.

Gale D. Rossides,

Acting Administrator.

[FR Doc. 2009-21794 Filed 09/15/2009 at 8:45 am; Publication Date: 09/16/2009]