DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Parts 1520, 1540, 1542, 1544, 1546, and 1548

[Docket No. TSA–2004–19515; Amendment Nos. 1520–4, 1540–7, 1542–2, 1544–5, 1546–2, and 1548–2]

RIN 1652–AA23

Air Cargo Security Requirements

AGENCY: Transportation Security Administration (TSA), DHS.

ACTION: Final rule.

SUMMARY: The Transportation Security Administration is amending its regulations to enhance and improve the security of air cargo transportation. This final rule requires airport operators, aircraft operators, foreign air carriers, and indirect air carriers to implement security measures in the air cargo supply chain as directed under the Aviation and Transportation Security Act. This final rule also amends the applicability of the requirement for a ''twelve-five'' security program for aircraft with a maximum certificated takeoff weight of 12,500 pounds or more to those aircraft with a maximum certificated takeoff weight of more than 12,500 pounds to conform to recent legislation.

DATES: *Effective Date:* This final rule is effective October 23, 2006.

Compliance Date: By November 22, 2006, Indirect air carriers must comply with the requirements for Indirect air carrier training under § 1548.11.

By December 1, 2006, aircraft operators, foreign air carriers, and indirect air carriers must comply with the requirements for—

Security threat assessments under §§ 1544.228, 1546.213, 1548.15, and 1548.16; and

Indirect air carriers that do not currently hold a security program under part 1548, and that offer cargo to an aircraft operator operating under a full all-cargo program or a comparable foreign air carrier under § 1546.101(e), establishment of, and operation under, a TSA security program in part 1548.

FOR FURTHER INFORMATION CONTACT: Tamika McCree, Office of Transportation Sector Network Management (TSA–28), Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202; (571–227–2632); *tamika.mccree@dhs.gov*.

SUPPLEMENTARY INFORMATION:

Availability of Rulemaking Documents

You can get an electronic copy using the Internet by—

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) Web page (*http://dms.dot.gov/search*);

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

(3) Visiting TSA's Law and Policy Web page at *http://www.tsa.gov* and accessing the link for ''Law and Policy'' 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 Preamble

AAAE American Association of Airport Executives
AAPA Association of Asia Pacific Airlines
ACCA Air Courier Conference of America
ACISP All-Cargo International Security Procedures
ACI–NA Airports Council International-North America
AEA Association of European Airlines
AES Automated Export System
ALPA Air Line Pilots Association International
AOPA Aircraft Owners and Pilots Association
ASAC Aviation Security Advisory Committee
ATA Air Transport Association
ATSA Aviation and Transportation Security Act
CAA Cargo Airline Association
CBP U.S. Customs and Border Protection
CFR Code of Federal Regulations
CHRC Criminal History Records Check
DHS Department of Homeland Security
DSIP Domestic Security Integration Program
EA Emergency Amendment
FAA Federal Aviation Administration
HAZMAT Hazardous Materials
IAC Indirect Air Carrier
IACSSP Indirect Air Carrier Standard Security Program
IATA International Air Transport Association
MSP Model Security Program
MTOW Maximum certificated take-off weight
NACA National Armored Car Association
NATA National Air Transport Association
NCBFAA National Customs Brokers and Forwarders Association
RAA Regional Airline Association
RACCA Regional Air Cargo Carriers Association
SIDA Security Identification Display Area
SD Security Directive
SSI Sensitive Security Information
STA Security Threat Assessment
TSA Transportation Security Administration
TFSSP Twelve-Five Standard Security Program
UPS United Parcel Service

Outline of Final Rule

I. Background

This final rule implements air cargo security requirements under the Aviation and Transportation Security Act (ATSA), Pub. L. 107–71. ATSA requires TSA to implement the following requirements:

- Provide for screening of all property, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft operated by a domestic or foreign air carrier;[1] and
- Establish a system to screen, inspect, or otherwise ensure the security of freight that is to be transported in all-cargo aircraft as soon as practicable.[2]

TSA published a notice of proposed rulemaking in the **Federal Register** on

[1] 49 U.S.C. 44901(a).

[2] 49 U.S.C. 44901(f).

November 10, 2004, at 69 FR 65258, to solicit public comment on the proposed air cargo regulations. Please see the NPRM for additional background information on the development of these regulations. The NPRM proposed, among other requirements, to:

- Address two critical risks in the air cargo environment: (1) The hostile takeover of an all-cargo aircraft leading to its use as a weapon; and (2) the use of cargo to introduce an explosive device onboard a passenger aircraft.
- Create a new mandatory security regime for aircraft operators and foreign air carriers in all-cargo operations using aircraft with a maximum certificated take-off weight more than 45,500 kg.
- Create requirements for foreign air carriers in all-cargo operation with an aircraft having a maximum certificated take-off weight more than 12,500 pounds but no more than 45,500 kg, and a separate program for aircraft with a maximum certificated take-off weight more than 45,500 kg.
- Require a Security Threat Assessment for individuals with unescorted access to air cargo.
- Enhance existing requirements for indirect air carriers (IAC).
- Expand Security Identification Display Area requirements at regulated airports to include areas where cargo is loaded and unloaded.

The NPRM was based in part on recommendations received from the Department of Transportation Office of Inspector General's (DOT OIG's) September 2002 audit of the air cargo security program,[3] the General Accounting Office's (GAO's) December 2002 report entitled, ''Vulnerabilities and Potential Improvements for the Air Cargo System'',[4] and the Aviation Security Advisory Committee recommendations of October 1, 2003. TSA was also guided by the Air Cargo Strategic Plan, which was completed in November 2003, and approved by the Department of Homeland Security in January 2004. The NPRM proposed a threat-based, risk-managed program for securing the air cargo transportation system.

This final rule adopts the regulations proposed in the NPRM with minor revisions to clarify certain provisions from the proposed rule. Specifically, the final rule clarifies both of the populations who are subject to Security Threat Assessments (STAs), and the areas where airports must extend Security Identification Display Area (SIDA) measures for cargo.

[3] Report Number SC–2002–113, September 19, 2002. This report is SSI.

[4] GAO–03–344, December 20, 2002.

During this rulemaking, another critical security enhancement has been implemented, that is, an increase in the inspection of cargo by aircraft operators and foreign air carriers. The NPRM proposed to codify the requirement for the aircraft operators and foreign air carriers to inspect cargo in accordance with their security programs. These operators already were inspecting a portion of their cargo as required by Security Directives issued by TSA in November 2003.

Following the publication of the NPRM, the Department of Homeland Security Appropriations Act, 2005 was enacted.[5] Section 513 of the Act requires TSA to amend Security Directives and programs to triple the percentage of cargo inspected on passenger aircraft, which TSA did. Details of these security measures are protected by TSA as Sensitive Security Information,[6] and therefore are not available for release to the general public.

Although the details are not in the rule, the regulatory evaluation for this final rule analyzes the cost incurred by aircraft operators and foreign air carriers to comply with this inspection requirement. The cost of inspection of air cargo on passenger aircraft accounts for about $1.491 billion of the total $2 billion costs of this rule, as discussed further in the Regulatory Evaluation Summary (Section V.A.) of this preamble. This inspection requirement accounts for the largest single cost of this final rule. This inspection requirement is not a new responsibility under this final rule; rather, TSA is taking this opportunity to provide a cost estimate for inspection of air cargo on passenger aircraft, as currently required under existing Security Directives. TSA provided cost estimates for these inspections in the NPRM, and has since revised them to account for the effect of the congressional directive and public comments. These Security Directives were first issued in November 2003. TSA subsequently issued security program amendments to reflect the inspection requirements of the Security Directives and the congressional mandates. These amendments have been implemented since July 2005. This rulemaking marks TSA's first opportunity to account for costs associated with the issuance of these security measures. The specific requirements for these inspections are SSI and are not appropriate for public disclosure as part of this rulemaking.

Accordingly, about 75 percent of the approximately $2 billion overall 10-year cost of the requirements implemented under this rule are associated with requirements that did not originate with this rule. These costs originated with TSA Security Directives issued in November 2003 and security program amendments issued in March 2005. The cost of implementing requirements that originate under this final rule is estimated to be about $167 million over a 10-year period.

In conjunction with the publication of this final rule, TSA is issuing to regulated parties for comment proposed amendments to their security programs to implement this final rule as authorized under 49 CFR 1542.105, 1544.105, 1546.105, and 1548.5.

[5] FY '05, Pub. L. 108–334.

[6] ''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.

II. Comment Disposition

TSA received 134 letters commenting on the NPRM. These comments were submitted by a broad cross-section of parties with an interest in air cargo security; including aircraft operators, foreign air carriers, trade associations, airports, state and local governments, and indirect air carriers (IACs).[7] These comments are addressed below, organized by major issues.

II.A. Security Threat Assessments (STAs)

TSA received approximately 140 comments on the proposed requirement for security threat assessments (STAs) for persons with access to air cargo. The STA proposed by TSA would include a search by TSA of domestic and international databases to assess any potential terrorist threats from those individuals with access to air cargo. TSA currently requires a variety of individuals working in aviation to submit to a criminal history records check and an additional name-based background check. Generally, these individuals work on airport grounds and have access to secure areas. However, many other persons who have not been subjected to such background checks have access to air cargo. TSA

[7] ''Indirect air carrier'' or ''IAC'' means any person or entity within the United States not in possession of an FAA air carrier operating certificate, which undertakes to engage indirectly in air transportation of property, and uses for all, or any part, of such transportation the services of an air carrier. This does not include the U.S. Postal Service (USPS) or its representative while acting on the behalf of the USPS. See 49 CFR 1540.5. This definition reflects an amendment pursuant to this final rulemaking.

proposed to require that STAs be conducted on additional categories of persons who have unescorted access to air cargo to verify that these individuals do not pose a security threat. Individuals who undergo security checks required for unescorted access to a security identification display area (SIDA), or who have successfully completed another STA that TSA approves as comparable, would not be required to submit to an STA.

Applicability and Definitions

Comment: The majority of comments addressing the proposed STA requirement expressed uncertainty about which employees would be required to have an STA, and what TSA considers to be ''unescorted access to cargo'' for purpose of triggering the STA requirement. In addition, the Regional Airline Association (RAA) states that the proposed language appears much broader than the scope previously recommended by the Aviation Security Advisory Committee (ASAC) because the requirement conceivably could apply to individuals who work outside of the airport environment. RAA believes that only individuals under the direct control of all-cargo airlines working at the airport should be subject to the STA requirement.

The National Air Transport Association (NATA) suggests that TSA clarify specifically which persons are covered by the STA requirement—either under this rule or by amendment to a security program—and which persons are excluded from the STA requirement. NATA states that because of industry confusion, a number of aircraft operators are unclear of their status with regard to the threat assessment requirement.

The Air Transport Association (ATA) commented that they fully support TSA's conclusion that it is not necessary to require every employee of an entity regulated by TSA that is in the business of cargo transportation to submit to an STA. However, ATA believes that the proposed language in §§ 1540.201 and 1544.228 is overly broad and subject to various interpretations.

ATA states that, as written, the rules could apply to individuals who work outside the airport perimeter in cargo storage facilities or holding areas, truck drivers, and others who move cargo to airports on behalf of shippers. ATA believes that the rule also could apply to individuals who work at non-U.S. locations and employees of entities at the airport who share space or have access to air cargo areas operated by the regulated party, such as employees of fixed base operators who provide fuel and other supplies to regulated parties. ATA states that such broad coverage would be impractical and disruptive to timely air cargo transport, and urges TSA to clarify the language to limit the applicability.

In addition, ATA recommends amending this section to apply to direct employees and authorized representatives of aircraft operators with unescorted access to cargo accepted by such aircraft operator. Federal Express (FedEx) recommends that TSA limit the STA requirement, to the extent permitted by applicable law, to employees who have unescorted access to the aircraft or cargo, or employees who they know or have reason to know will have access to cargo that will be tendered to a passenger carrier to be flown on a passenger aircraft.

A number of comments asked for clarification as to what other security checks are approved by TSA, and, thus, would not require completion of an STA for that individual.

TSA response: TSA agrees that not every employee should be subject to the STA requirement. Instead, TSA requires an STA for employees and agents of aircraft operators, foreign air carriers, and IACs who have unescorted access to cargo at certain times. TSA also requires an STA for certain IAC principals. TSA has revised the provisions of the regulations to clarify the STA requirement. While these revisions comport with the scope of the NPRM, we have restructured the sections to indicate more clearly which personnel are required to meet the STA requirements. The revisions clarify that the STA requirements apply:

- Only in the United States.
- To aircraft operators with a full program, or a full all-cargo program; foreign air carriers under § 1546.101(a), (b), or (e); and indirect air carriers.
- To individuals with unescorted access to cargo who are employees or agents of—[8]
- Aircraft operators with a full program and foreign air carriers under § 1546.101(a) or (b) where they accept cargo;
- Aircraft operators with a full all-cargo program and foreign air carriers under § 1546.101(e) where they consolidate or inspect cargo;
- IACs which accept cargo for transportation on aircraft operated by an aircraft operator with a full program, or a foreign air carrier under § 1546.101(a) or (b); or
- IACs where they consolidate or hold cargo for transportation aboard an aircraft operated by an aircraft operator with a full or full all-cargo program, or a foreign air carrier under § 1546.101(a), (b) or (e).
- Unless the employee or agent has a Criminal History Records Check (CHRC) for unescorted authority to a SIDA, or another STA approved by TSA as comparable to an STA under subpart C.

It is helpful to note where employees and agents are not required to have an STA. Appropriate background checks for access to airport-restricted areas are obligatory under International Civil Aviation Organization (ICAO) Annex 17 Standards. TSA does not require STAs for unescorted access to cargo at foreign locations.

Individuals do not need an STA if a person with the appropriate background check escorts them. Individuals who work near cargo, but do not require unescorted access to cargo, do not need an STA where the regulated entity has adopted access control measures to prevent unescorted access to the cargo. TSA will provide guidance on specific access control measures in their security programs and regulated entities may work with TSA to establish additional measures for TSA approval.

Ensuring that individuals are properly escorted, or that cargo is in a locked, inaccessible area, are two of many possible examples of access control measures that may be available to regulated entities. Generally, TSA relies on the access control measures that have been in place through FAA and TSA regulations for many years. Regulated entities should contact their TSA principal security inspectors, or other appropriate TSA point of contact, if they have further questions regarding access control measures.

Where employees and agents subject to STA requirements have successfully completed a CHRC for unescorted access authority to a SIDA, they have met their requirement and do not need to get a separate STA under this final rule. TSA already requires airport operators to send to TSA certain personal information for each individual who has undergone a CHRC for a current SIDA or sterile area ID in order to perform an additional background check that is comparable to an STA.

TSA is providing instruction to aircraft operators with a full or full-all-cargo program to send to TSA the same type of information for cargo screeners who do not have current SIDA or sterile area IDs, and will also perform the additional check on this population. Most of these cargo screeners already

[8] The STA requirements also extend to an officer, director, and person who holds 25 percent or more of total outstanding voting stock of an IAC. However, TSA did not receive requests for clarification to this requirement.

have SIDA IDs; and, thus, already are checked. Likewise, an employee or agent who has undergone another STA that TSA approves as being comparable does not need a separate STA under this rule. TSA considers the threat assessments it conducts for a person holding a commercial driver's license with a hazardous materials endorsement as comparable to an STA for purposes of this rule. *See* 49 CFR part 1572. TSA may determine that other threat assessments are comparable to the STA requirement under this rule and will expressly notify regulated entities with security program amendments from TSA upon making that determination. An employee or agent authorized to engage in the actions described below, who does not meet one of these means of compliance, must obtain an STA as directed in part 1540 of this rulemaking.

For cargo accepted by an aircraft operator with a full program and a foreign air carrier under § 1546.101(a) and (b), each employee or agent, whom the operator authorizes to have unescorted access, must have an STA.[9] The STA requirement for these employees and agents applies at the point of acceptance, whether from a shipper, another aircraft operator, foreign air carrier, or indirect air carrier.

For cargo accepted in the United States by an aircraft operator under a full all-cargo program, or a foreign air carrier under § 1546.101(e), this provision applies to each employee or agent authorized to have unescorted access to cargo from the time the regulated entity consolidates or inspects cargo until it is loaded on an aircraft. TSA has determined that security procedures for these all-cargo operations are best focused, and more efficiently applied, at locations where cargo is consolidated or inspected. Reasons for this determination include the layered security approach and the focus on interdicting stowaways.

STA requirements for IAC employees and agents parallel measures from both passenger and all-cargo aircraft operators. Each IAC employee or agent who has unescorted access to cargo for transportation on a passenger aircraft must have an STA. For transportation aboard an all-cargo aircraft, each IAC employee and agent must have an STA, if the IAC authorizes them to have unescorted access to cargo, from the time the cargo reaches an IAC facility where the IAC consolidates or holds the cargo.

[9] Employees and agents do not need this STA if they have successfully completed a background check for unescorted access to SIDA, or have another threat assessment that TSA approves in this context.

Comment: A few commenters note that there seems to be a conflict between proposed § 1540.201 and proposed § 1544.228; specifically, proposed part 1544 includes a provision of applicability of STAs to operators, but part 1540 does not. The commenters request that TSA clarify the scope of these sections, recognizing that the exclusion of all-cargo operators from § 1540.201 may have been inadvertent.

TSA response: TSA's omission of aircraft operators under a full all-cargo security program in § 1540.201(a)(1) was an oversight. We have provided a technical amendment to that subparagraph, adding ''or (h)'' to the end of the provision.

Operators' Responsibility

Comment: The Air Line Pilots Association International (ALPA) does not support the STA requirement because ALPA favors requiring persons with unescorted access to cargo to submit to a CHRC. ALPA argues that under the proposed rules, TSA could approve for unescorted access to air cargo an individual convicted of any of the 28 defined crimes because his or her name does not appear on government-maintained lists of individuals suspected of having a link to terrorism. ALPA states that criminal history, financial status, and many other factors can be indicators of an individual's character, reliability, maturity, and susceptibility to compromise.

TSA response: TSA recognizes that there are a number of background check techniques that potentially could be applied to various persons in the supply chain. In accordance with our risk based, threat managed approach; TSA has determined that requiring persons with unescorted access to cargo to submit to an STA provides a significant enhancement while limiting costs. We note that persons with more sensitive positions, such as cargo screeners, are subject to CHRCs and additional background checks.

Comment: Federal Express (FedEx) states, that in many cases, it would be unlawful for operators to conduct background checks on persons not directly employed by them. FedEx recommends requiring an operator to conduct such checks only on its direct employees. FedEx also expresses concern about requirements to have STAs for agents due to possible labor and employment law issues.

FedEx also commented that for an IAC to fulfill this requirement, it will have to maintain employee records for all the truckers and warehousemen used by the IAC. Further, IACs will have to ensure that their vendors provide them timely updates of changes in employment and monitor unescorted access to cargo. FedEx believes that for the majority of IACs this would be an impossible task.

Another comment supports the proposed section, but asserts that carriers should not be responsible for completing third party STAs. The commenter asserts that each entity should be responsible for completing its own STAs, and TSA should be responsible for funding any new background checks.

TSA response: Aircraft operators, foreign air carriers, and IACs are responsible for carrying out all security measures as regulated parties. They do so using employees and agents, as they choose. They authorize unescorted access to cargo by agents and employees. Under these regulations, however, these regulated parties are not responsible for conducting the required background checks; rather they must ensure that the necessary information about their employees and agents is transferred to TSA for TSA to conduct the STA.

TSA has carefully examined the scope of the need for an STA. TSA has revised the language of proposed §§ 1544.228, 1546.213, and 1548.15 to pertain to those individuals specifically authorized to have unescorted access to cargo. This final rule provides the aircraft operator, foreign air carrier, and IAC latitude in authorizing unescorted access to cargo in order to limit the number of persons requiring an STA. The requirement for an STA does not extend to employees or agents who are only near air cargo where the aircraft operator, foreign air carrier, or IAC has in place other security measures to control access to the cargo.

If a regulated entity uses a third party agent to meet its security program requirements, which regulated entity is responsible for ensuring that the third party has an STA, just as they are responsible for other security duties their agents carry out. TSA is aware of no conflict with other laws with regard to collecting STA information.

Comment: National Armored Car Association (NACA) states that requiring additional background checks on employees, who have already been investigated and certified by State agencies charged with licensing security personnel, is redundant and wasteful. NACA suggests that TSA accept certifications based on State investigations which include FBI fingerprint examinations, and issue any necessary TSA credentials based on these background checks.

The American Trucking Association states that placing direct responsibility on operators to perform STAs on their agents, contractors, or subcontractors places a substantial financial burden on the operator and driver, and potentially will create a confusing, frustrating, and unworkable system.

Other concerns of the American Trucking Association include whether STAs are transferable (i.e., would follow the employee as he or she changes employment), and how often individuals are required to renew their security authorization. The American Trucking Association proposes the use of TSA's Transportation Worker Identification Credential as an alternative solution to implementing STAs on individuals having unescorted access to air cargo.

TSA response: In general, TSA does not anticipate accepting the background check of a private company or a state agency as comparable to a CHRC or STA approved by TSA. The TSA STA checks intelligence databases that are inaccessible to the private sector and not widely used by state agencies. As mentioned under § 1540.201, STA requirements apply to those aircraft operators, foreign air carriers, and IAC employees and agents who are authorized and required to handle air cargo in the performance of their duties. STA requirements do not apply to employees and agents who have only incidental access to air cargo, or employees and agents who are required to submit to another TSA-approved STA, such as TSA HAZMAT driver's license requirements.[10] TSA will consider accepting other TSA-approved STAs, such as the Transportation Worker Identity Credential upon broader implementation of its use.

Consistent with TSA policy on transferability of a CHRC conducted for unescorted access authority to a SIDA, an employee or agent who has successfully completed an STA for one employer need not complete it for another employer if the employee or agent has been continuously employed in a position that requires an STA. Additionally, as detailed in the response to the first comment on 'Notification' below, there is no requirement to renew an STA as long as the STA-holder qualifies as continuously employed. TSA will provide further guidance to aircraft operators, foreign air carriers, and indirect air carriers upon request.

[10] See 70 FR 22268 (Apr. 29, 2005), to be codified at 49 CFR part 383.

Notification

Comment: Several commenters note the potential lengthy turn-around time for STA notifications under § 1540.205 and recommend that TSA include a time frame in which it will make the notification. Many of these commenters propose that TSA should specify an anticipated response time of 10 working days to provide authorization or initial denial to submitted STAs. One commenter notes that TSA will need to increase staffing to handle the impact of processing the STAs in a timely manner.

The American Trucking Association commented that the proposed rule excludes certain employers from receiving STA results on their drivers. Without employer notification, trucking companies are unable to make informed personnel decisions regarding their drivers. The American Trucking Association recommends amending this section to include notification to the individual, operator, and employer.

TSA response: TSA agrees that an anticipated response time of 10 working days in providing authorization or initial denial is appropriate and achievable in most cases. While some individual situations may require a longer timeframe for adjudication, TSA should provide the vast majority of approvals well within 10 working days. TSA further notes that once it approves an STA, by issuing a ''Determination of No Security Threat'', the STA will remain valid for an employee or agent from one job to another in accordance with §§ 1544.228(b)(2), 1546.213(b)(2), and 1548.15(b)(2), and consistent with TSA policy on continuous employment for holders of unescorted access authority to SIDA. However, TSA notes that the regulated party and the agent's direct employer are not prohibited from communicating about the notification.

Appeals Procedures

Comment: The Airport Consultants Council proposes new language to clarify the requests for materials under the appeals procedure of § 1540.207(c)(1).

TSA response: Rather than adopt new language, TSA revised § 1540.205(c)(4) by adding a cross-reference to § 1540.207. Section 1540.207(c) allows an appeal, including a written request for materials, within 30 days of receipt of the ''Initial Determination of Threat Assessment'' from TSA.

STA Fee

Comment: United Parcel Service (UPS) states that they already conduct extensive background checks, including checking all airline employees against Federal governmental watch lists. If the TSA check merely duplicates what the air carrier already is doing, UPS contends there is no need for TSA to conduct the test and for the air carriers to pay the fee under § 1540.209. UPS suggests that if TSA wants additional name checks with the proposed STA, then TSA should add the additional checks to the current listings and let the air carriers run them. This method does not place additional costs on TSA or the air carrier because the programming and personnel already are in place.

Additional commenters request clarification on the procedures involved in an STA, because they do not understand the nature of the analysis or the basis of the $39 cost figure in the NPRM. The commenters believe that the proposed cost for the STA is excessive, given the cost of the comparable and more extensive CHRC checks.

The Air Courier Conference of America (ACCA) and Purolator Courier oppose the fee, and state that TSA should carefully define the applicable population before it requires any new screening. They recommend that TSA conduct the screening against watch lists and the National Crime Information Center.

FedEx states that, the new STA program will, contrary to TSA's expectations, increase both direct and indirect costs. They state that the direct cost of $39 for each STA is significantly more than the average cost of a CHRC. In addition, FedEx contends that the name-based methodology of an STA will result in indirect costs resulting from operational delays and disruptions due to false positives. FedEx argues that such indirect costs will exceed those that currently result from the CHRC.

Like UPS, FedEx believes that air carriers should not have to pay TSA or another party to do something that they are already doing. The International Air Transport Association (IATA), Yellow Roadway, British Airways, Delta, and other commenters oppose the fee proposed in this section and believe that it is the Government's responsibility to provide protection from terrorists and to absorb any costs related to the STAs.

TSA response: Private companies do not have access to all of the intelligence databases that TSA will use to conduct STAs. Further, TSA must make judgments as to the information received from the databases, which it has the expertise to apply. Accordingly, TSA has decided to conduct the STAs. Statutory provisions [11] require that

[11] Department of Homeland Security Appropriations Act, 2004, Sec. 520 (Pub. L. 108–90, Oct. 1, 2003, 117 Stat. 1137).

industry should reimburse the agency for direct costs associated with accomplishing STAs. The STAs will not duplicate checks that the carriers are already accomplishing, as TSA has access to a variety of Government watch lists that are not appropriate for dissemination to the private sector. The $39 fee referenced in the NPRM assumed TSA would need to pay the FBI for access to the FBI's Automated Case System files. Subsequent to NPRM publication, TSA decided not to include the Automated Case System component in its STA. With increased vetting and credentialing experience, TSA has refined the necessary threat assessment sources to be included. As a result, the revised STA fee is $28.

The rule provides for a phased-in implementation for compliance with the STA requirements. Regulated entities may mitigate delay in processing by timely submitting the STA application. Subsequent to the compliance date, any possible delay due to a false positive would occur prior to the applicant's authorization to have unescorted access to cargo. These new hires would constitute a small portion of the entire population subject to the STA. TSA expects that the percentage of false positives among these new hires will be minimal. Further, TSA analysts will be able to resolve most false positives quickly within the anticipated time frame for returning results.

Section 1546.213 STAs for Cargo Personnel in the United States

Comment: Japan Airlines wants TSA to clarify whether this section would require foreign air carrier employees to undergo STAs or other checks when accessing off-airport facilities, despite the non-application of SIDA-like requirements to such facilities. Nippon Cargo Airlines asks if the rule will apply only to new employees or if it will affect existing employees.

TSA response: Foreign air carrier employees and agents within the United States are subject to the same requirements off-airport as corresponding U.S. aircraft operator employees and agents.

If the foreign air carrier authorizes its employee or agent to have unescorted access to cargo at an off-airport facility and this facility is used to consolidate or inspect cargo until it is loaded on the aircraft, or an employee or agent accepts cargo from a known shipper, then the requirements of § 1546.213 apply. The requirements apply to both new and existing employees and agents who have unescorted access authority granted by the foreign air carrier.

Section 1548.15 STAs for Individuals With Unescorted Access to Air Cargo

TSA received 15 comments on this section. Most commenters have doubts about the responsibilities of IACs regarding this rule. They want to know who will need the STA and whether the requirements are retroactive for current employees.

Comment: Atlanta-Hartsfield International Airport (ATL) asks if this requirement includes personnel in the manufacturing and shipping phase of preparing air cargo, and if so, whether an IAC will be responsible for filing an STA application on each loading dock employee and transport driver in the shipping chain. ATL also asks if these requirements are retroactive for current IAC employees or other cargo related businesses, and if so, for how many years into the past and how soon will the applications need to be filed.

TSA response: The STA requirements apply to those aircraft operator, foreign air carrier, and IAC employees and agents who are authorized to have unescorted access to air cargo in the performance of their duties. Manufacturing or shipping personnel would only be required to have an STA if they are acting as an agent and have unescorted access to cargo for an aircraft operator, foreign air carrier, or IAC.

Current IAC employees and agents are required to complete an STA successfully. TSA is providing 180 days from the date of publication of this rule for aircraft operators, foreign air carriers, and IACs to comply with the STA requirements.

Comment: Air Courier Conference of America (ACCA) asks to which employees this section will apply, and why some employees will need to undergo a background check against TSA's lists while others may undergo a CHRC. They note that most ACCA members already check employee names against the ''no fly'' and ''selectee'' watch lists as a standard element of their Security Directives, and as an added safeguard.

TSA response: This rule requires STAs within the United States for employees and agents authorized by aircraft operators, foreign air carriers, and indirect air carriers to have unescorted access to cargo. Persons who have CHRCs for unescorted access authority to a SIDA already have undergone TSA name-based checks comparable to the STA and therefore will not have to undergo another one.

Comment: ATA supports a reasonable extension of STAs for IACs, but warns of significant potential for system disruptions, unless TSA defines IAC and air carrier responsibilities with regard to STA clearance. ATA asserts that air carriers cannot be responsible for ensuring the clearance of each IAC handler who may have contact with cargo before the delivery to the air carrier. ATA believes that this is not a workable process given the inherent time sensitivities in air cargo transport, the number of IACs providing cargo to air carriers, and the nature of an IAC's workforce scheduling.

TSA response: TSA inspectors verify IAC compliance with STA requirements in the normal course of regulatory compliance inspections. Air carriers are not required to verify the IAC's compliance as part of the air cargo acceptance process.

Comment: National Customs Brokers and Forwarders Association (NCBFAA) questions whether longtime employees, and licensed customs brokers, many of whom are also IACs and certified by U.S. Customs and Border Protection (CBP) under the Customs-Trade Partnership Against Terrorism program (C–TPAT), are subject to STA requirements. NCBFAA believes that these employees have proven their reliability and conscientiousness on security matters and it would be inefficient and unnecessary to subject them to background checks. NCBFAA recommends that TSA either exempt individuals previously approved by the CBP, or work with CBP to harmonize their respective screening processes. NCBFAA also proposes that TSA exempt IAC employees with a certain level of experience. NCBFAA believes it would be redundant to require a second DHS screening for many IAC employees. In addition, the NCBFAA recommends that TSA limit STA screening to a five-year period for persons who remain in good standing.

TSA response: TSA will not exempt any employee from STA requirements based on length of service. TSA believes that performing background checks on individuals playing critical roles in the air cargo supply chain is a necessary step in ensuring aviation security. TSA currently is working with other DHS components to consider background checks performed by those components to determine if they are comparable to checks performed by TSA. Regulated entities will be able to refer to their security programs as provided by TSA for information on comparable checks. Regulated entities have incentive to determine whether an applicant has already completed a comparable check because the employee would not have to wait for clearance for unescorted access to cargo. Also TSA is providing in security programs that regulated entities

must accept the comparable check in lieu of the STA.

II.B. Acceptance and Screening of Cargo

Comment: The majority of commenters on §§ 1544.205, 1546.205, and 1548.9 regarding inspection and screening of cargo are not sure how to accomplish compliance.

TSA response: Specific Sensitive Security Information (SSI) measures will be proposed as amendments to airport, aircraft operator, foreign air carrier, and IAC security programs. The contents of these programs are not appropriate for public disclosure as part of this rulemaking. TSA is providing airport operators, aircraft operators, foreign air carriers, and IACs the opportunity to comment on the proposed amendments to their security programs upon issuance, and before the effective date of this final rule. It is helpful to note that many of these measures already appear in current Security Directives and security program requirements.

Comment: UPS, ATA, Regional Airline Association (RAA), and Cargo Airline Association (CAA) state that § 1544.205(a) and (b) are imprecise and redundant, and propose alternative language to consolidate the paragraphs.

TSA response: Paragraph (a) of § 1544.205 provides the general requirement and performance standard for carriage of cargo. Paragraph (b) provides the specific requirement for screening and inspecting cargo. Other paragraphs provide other specific requirements. The revision also extends those requirements to all-cargo aircraft operations with a maximum certificated take-off weight (MTOW) of more than 45,500 kg (100,309.3 lbs.). These paragraphs do not provide details of how these requirements must be met, because such details are Sensitive Security Information under 49 CFR part 1520 and are contained in security programs that are available only to persons with a need to know.

Comment: Several commenters oppose requiring regulated entities to refuse cargo for transport if the shipper does not consent to screening and inspection of the cargo under §§ 1544.205(d) and 1546.205(b). They state that high cash value cargo, such as jewelry, currency, bullion, and other sensitive cargo, is shipped in sealed containers that cause damage or losses to cargo when opened. They suggest additional consideration and industry input on how to deal with these situations and ask whether the Government will provide indemnification if damage occurs during inspection by the Government or Government contractor personnel.

TSA response: Regulated entities must refuse to transport cargo as required under, and consistent with, their security programs. TSA understands that requiring shippers, like drug companies, to consent to inspection of cargo is problematic. TSA agrees that the screening of certain types of cargo present unique challenges, and recognizes the safety and security concerns related to screening such cargo. TSA revised the wording in sections that require consent to screen cargo, and provides specific exceptions and alternative procedures in the proposed security program amendments for shipments whose contents would be damaged or compromised if the aircraft operator inspected the cargo. These procedures largely will be transferred from current Security Directives that address these concerns for later consideration in amendments to applicable security programs.

Comment: NACA and NATA ask if the terms ''inspect'' and ''screen'' are interchangeable.

TSA response: The terms ''inspect'' and ''screen'' are not interchangeable. Generally, screening means the systematic evaluation of a person or property to assess whether either poses a threat to security. TSA interprets inspection as a subset of screening. An inspection is a method of conducting such an evaluation, but is not the only method. For instance, the known shipper program is an information-based method of screening. The known shipper program involves the screening of cargo based upon information known to an aircraft operator, foreign air carrier, or indirect air carrier about the shipper of the cargo. Additionally, a certain percentage of that cargo is inspected for the presence of persons and any unauthorized explosives, incendiaries, and other destructive substances or items.

TSA will provide specific guidance to regulated entities in their respective security program amendments.

Comment: FedEx wants TSA to clarify that the proposed rule does not require or authorize TSA to impose any additional screening beyond the screening they already are doing under SDs and security program amendments. Several all-cargo air carriers ask if TSA will bear the costs of the screening workforce and equipment required under § 1544.205, and want TSA to clarify who has the responsibility for screening cargo.

TSA response: Aircraft operators incur the cost for the screening of cargo transported aboard their aircraft and must comply with the procedures for screening incorporated in their security programs. Specific screening requirements are promulgated in amendments to such programs and regulated parties are provided the opportunity to comment on these amendments, as appropriate.

Regarding screening of cargo for transportation aboard passenger aircraft, 49 U.S.C. 44901(a) provided an exception for Federal screening for the known shipper program. The inspection of a portion of known shipper cargo is considered a part of the known shipper program and need not be conducted by Federal employees. This rule does not address the amount or type of cargo screening that is required. TSA will respond to changing conditions as needed. Additionally, TSA is considering whether the current system for selecting cargo for inspection will be changed with the TSA Freight Assessment System (FAS). The FAS might be used to identify cargo posing an elevated risk for the application of security measures in the aircraft operator's security program.

Comment: FedEx, UPS, CAA, and ATA note that § 1544.205(e) appears to prohibit the acceptance of cargo for air transportation from a variety of retail outlets, such as the UPS Store, FedEx, Kinko's, and other authorized shipping outlets. The commenters note that these outlets are neither the shipper nor an entity specifically mentioned with a comparable security program under § 1544.205(e). However, the commenters believe that the exception under § 1544.205(e) will permit them to continue to accept cargo from these retail outlets as is currently allowed in their security programs. The commenters want TSA to clarify that this is, in fact, TSA's intention. Further, if this is not the intention of TSA, they recommend excluding carriers operating under all-cargo programs from the application of this section, and propose using the following language for § 1544.205(e): ''Each aircraft operator operating under a full program or an all-cargo program may accept cargo for air transportation on a passenger air carrier only from a known shipper, or from an aircraft operator, foreign air carrier, or IAC operating under a security program under this chapter with a comparable cargo security program.''

TSA response: Aircraft operators under a full all-cargo security program are not prohibited from accepting cargo from retail entities as described in these comments. Under these rules, such retail outlets may operate either under an IACSSP, or as an agent with security responsibilities under the aircraft

operator's security program. For a further discussion of the differences between IACs and agents of aircraft operators, please see the Section-by-Section Analysis for § 1548.5.

Comment: UPS, CAA, ATA, and others commenters express concern about the extraterritorial applicability of § 1544.205(f). CAA states that the rule seems to apply to international air cargo movements and notes that commercial realities and foreign government resistance make the application of this rule unattainable. UPS wants TSA to clarify this section to recognize that foreign law may limit the extent to which carriers may be able to comply with security programs outside the United States. ATA states that foreign countries may impose screening requirements that differ and even conflict with those in the carrier's security program and recommends that TSA permit air carriers to comply with either the security programs imposed by the foreign country or those contained in the TSA-approved security program.

TSA response: TSA recognizes, as indicated by the commenters, that the imposition of regulatory requirements on a U.S. aircraft operator operating from foreign locations may be impacted by the legal requirements applied by the host government at such foreign locations. The requirement for a U.S aircraft operator to screen cargo at foreign locations is no different from any other current or proposed aviation security requirement placed upon a U.S. aircraft operator operating outside the United States. The specific security program mandates for the screening of cargo outside of the United States take into consideration cargo security restrictions, as well as requirements mandated at some foreign locations.

Comment: Several smaller air carriers state that they cannot comply with the proposed rule requirement to open packages before loading at unsecured airports.

TSA response: This rule codifies requirements for screening that already are in place through SDs and security program amendments. The fact that an aircraft operator operates at an airport without a security program has not been found to inhibit screening.

Comment: Several airport operators and air carriers ask how to accomplish screening at rural airports.

TSA response: Each aircraft operator and foreign air carrier security program must take into consideration the different locations at which cargo must be screened. Aircraft operators and foreign air carriers must conduct screening at rural airports in accordance with the specific requirements of their security programs.

Acceptance and Screening of Cargo From Locations Outside the United States

Comment: Association of Asia Pacific Airlines (AAPA), British Airways, Association of European Airlines (AEA), and Singapore Airlines state that § 1546.205 lacks provisions regarding the acceptance and recognition of National Aviation Security Program requirements that many foreign airlines use. They recommend standardizing requirements for acceptance and screening of cargo, and implementing threat-based measures for inspection of cargo.

TSA response: TSA continues to recognize National Aviation Security Programs of foreign countries in accepted security programs.

Comment: Several commenters, including British Airways, IATA, and AEA want TSA to clarify the term comparable security program in § 1546.205(e), and ask what this term includes. In addition, these commenters recommend amending § 1546.205(f) to clarify that it applies only to cargo loaded outside the United States that is destined for the United States and that foreign air carriers may accept cargo destined for the United States from any lawful entity, subject to a compatible National Aviation Security Program as approved by the carrier's national government.

TSA response: A comparable security program includes cargo security measures identical or equivalent to those required of the accepting aircraft operator or foreign air carrier. If the transferring aircraft operator, foreign air carrier, or IAC, has performed these cargo security measures, there is no further need for the accepting aircraft operator or foreign air carrier to repeat those measures. For instance, for transfers to aircraft operators with a full program, TSA will consider such security measures as: Whether the known shipper program was applied, from whom the operator accepted the cargo, the type of cargo screening or inspection that was done, and other relevant security measures.

Overall, part 1546 applies to the operation, landing, or taking off within the United States of a foreign air carrier. Only cargo destined to, or transported through, the United States is subject to this final rule when loaded at a foreign airport. Section 1546.205(f) requires that foreign air carriers subject to this part carry out the requirements of their security programs. Section 1546.101 applies where a foreign air carrier lands or takes off in the United States.

Acceptance of Cargo by an Indirect Air Carrier

Comment: Most comments to § 1548.9 support this section and recommend that TSA allow IACs to screen cargo provided they demonstrate the capability to do so. The Yellow Road Corporation expresses concerns about the costs and redundancy associated with enforcing cargo security requirements for IACs, and recommends the adoption of varying levels of cargo screening with emphasis on loading cargo on the aircraft. IBM wants clarification on the requirement to obtain the shipper's consent to search or inspect cargo, and suggests allowing the shipper to give a blanket authorization to the IAC as part of its contract.

TSA response: While TSA does not state in which manner the shipper's consent to search or inspect cargo be obtained, it does require that the consent be explicit and in writing. TSA allows aircraft operators, foreign air carriers, and IACs to manage the collection of consent to search in a manner consistent with individual operational needs. The regulations allow a shipper to provide a blanket authorization, as proposed by IBM.

II.C. Security Identification Display Area (SIDA)

Comment: American Association of Airport Executives (AAAE) disagrees with TSA's assessment that airports easily will be able to extend SIDAs to areas where cargo is loaded and unloaded under § 1542.205. AAAE states that the rule does not adequately address the complexities of expanding SIDAs at airports with diverse operational configurations, property ownership, and jurisdictional control.

Aircraft Owners and Pilots Association (AOPA) states that while this rule may not impose direct mandates for general aviation areas at airports regulated by TSA under 49 CFR part 1542, AOPA is concerned that the practical implementation of this requirement will result in SIDA requirements in many general aviation areas. In addition, AOPA notes that many airports specifically exclude general aviation areas from the SIDA because of time and distance separation from the air carrier areas. This layered approach to security limits access points and the number of individuals needing the background check and identification requirements for the SIDA, and establishes clear distinctions of security areas.

AOPA recommends using the standard of the operational area of the aircraft principle for air cargo operations at part 1542 regulated airports, similar to that proposed for operations at non-part 1542 TSA regulated airports. AOPA further states that the operational area of the aircraft should include the immediate footprint of the cargo aircraft and handling area, with a procedure to limit unauthorized persons near the aircraft while it is being loaded and unloaded, but not the entire ramp.

The Department of Transportation of Alaska states that this final rule will require CHRCs for most people working at an airport, and contends that expansion of the CHRC requirement will not effectively increase security for air cargo.

TSA received some comments that relate to the fact that areas designated as SIDAs primarily are subject to airport operator control rather than aircraft operator control.

CAA states that expansion of the SIDA is not the best way to secure the area surrounding cargo aircraft. It further asserts that the ASAC Working Groups did not recommend such a SIDA expansion, but rather recommended the imposition of SIDA-like requirements on air carriers operating from these cargo areas. CAA, UPS, DHL, and FedEx comments that the difference is significant from an operational, but not a security, standpoint, noting that it is essential that the all-cargo air carriers retain access control so they can carry out their requirements and internal company procedures. CAA recommends requiring air carriers to amend security programs to include SIDA-like measures at non-SIDA operational areas of U.S. airports where cargo is loaded or unloaded from aircraft.

FedEx states that this section extends SIDA requirements to areas where operators sort loaded or unloaded cargo on airport grounds. However, § 1542.205(a)(2) does not contain this important language. FedEx recommends adding the phrase ''on airport grounds'' after every reference to ''each area'' in the rule to clarify that facilities such as FedEx stations, world service centers, and non-airport sort locations are not to be included in SIDAs. UPS also proposes extensive revisions to this section.

Airports Council International–North America (ACI–NA), ATA, and RAA do not support the extension of SIDA requirements. They state that the language is very broad and could potentially extend SIDA requirements far beyond what is necessary to ensure air cargo security. They recommend amending the SIDA requirements only to airport areas used to load or unload cargo from aircraft.

The Miami International Airport, Atlanta-Hartsfield International Airport, ACI–NA, and the Airports Consultants Council agree that the new requirement will enhance the overall level of security, but only if designated in those areas under airport control. They argue that the SIDA should begin at the wall of the cargo facility adjacent to the airside ramp locations. The commenters also oppose requiring airports to extend, or enforce the security of the SIDA into tenant-leased facilities.

Eleven small aircraft operators, AOPA, and Regional Air Cargo Carriers Association (RACCA) express concern about extending SIDA to cargo operating areas. The commenters state that the SIDA extension is impractical for aircraft operating under the TFSSP, since operations are conducted on common public areas like the general aviation and FBO ramps, and it would be impossible to extend SIDA requirements to these areas. The Juneau International Airport asks to designate dual use areas that are SIDA only during times that the cargo activity is performed, and asks if SIDA need to be contiguous. The Anchorage International Airport recommends allowing the local FSD to determine which areas, if any, need to be classified as SIDAs.

TSA response: TSA has determined that measures to prevent individuals from gaining unauthorized access to the cargo operations area are necessary to prevent tampering with the aircraft or the cargo and to remove a potential access point for stowaways. TSA considered requiring aircraft operators and foreign air carriers in all-cargo operations to implement SIDA-like requirements. However, TSA has determined that airport operators with security programs under 49 CFR 1542.101(a) are able to implement more efficiently the requirements to extend SIDAs.

These airports are better positioned with the necessary infrastructure to provide security measures, as they are able to leverage the existing resources that support SIDAs currently in place. Airports also will be able to rely on, or more easily expand, existing identification media and security check capabilities, law enforcement support, and training programs.

TSA considered limiting the extension of SIDAs to areas of a ramp where cargo is loaded or unloaded from the aircraft. However, the inside of facilities where cargo is sorted, stored, staged, consolidated, processed, screened or transferred, present numerous, and perhaps more, opportunities for someone to tamper with the cargo just before it is loaded onto an aircraft.

TSA also considered extending the SIDA requirement for similar cargo areas off-airport. TSA determined that the complexity and cost of applying these measures off-airport would be too great because they lack existing resources to expand. These off-airport locations would disproportionately incur significant start-up costs.

Accordingly, the final rule provides that SIDA security measures must be extended to secured areas and air operations areas that are regularly used to load cargo on, or unload cargo from, an aircraft operator under a full or full all-cargo program as provided in § 1544.101(a) or (h), or under a foreign air carrier program under § 1546.101(a), (b), or (e). Adoption of a security program under these sections applies to operation of an aircraft with an MTOW of more than 45,500 kg (100,309.3 lbs.). The requirements do not extend to areas used by aircraft with an MTOW of more than 12,500 lbs., but not more than 45,500 kg (100,309.3 lbs.).

Additionally, the SIDA security measures must be extended on an airport to areas where cargo is present after an aircraft operator, foreign air carrier, or indirect air carrier accepts cargo. In particular, this includes inside buildings such as cargo facilities, loading and unloading vehicle docks, and other areas where an aircraft operator, foreign air carrier, or indirect air carrier stores, stages, consolidates, processes, screens, or transfers cargo. As clarified in § 1542.205(a)(3), the SIDA is not required to include access routes between the perimeter entry point of the airport and the cargo facility, or one of these other locations, for the purpose of transporting cargo to or from an aircraft operator, foreign air carrier, or indirect air carrier.

There may be areas within a cargo facility that do not need to be SIDAs. For example, some parts of cargo facilities are not restricted to employees and agents of an aircraft operator, foreign air carrier, or indirect air carrier. These areas may have a counter where one of these operators accepts cargo from shippers, or the shipper's agents. The area leading up to this counter need not be a SIDA if there is no cargo in these areas that already has been accepted. Additionally, on a limited basis other security measures, such as access control measures or active and continuing surveillance or monitoring, may mitigate the need for SIDA in areas where an operator's customer or the

customer's agent is present to tender cargo.

Each airport security program will specify the actual limits of the cargo operations area to be included in a SIDA, subject to review and approval by TSA. Amendments to security programs may address the particular circumstances of an airport's layout and operations and accommodate other aviation operations to the extent practical. Note that under § 1542.111, an aircraft operator or foreign air carrier may enter into an exclusive area agreement with an airport operator to take responsibility for the SIDA.

Additionally, under § 1542.111 TSA encourages airports to grant an aircraft operator's request to enter into an exclusive area agreement for the inside of a building of any cargo facility on its airport where cargo is present after the aircraft operator accepts the cargo. For example, TSA recognizes that some aircraft operators may have buildings that house their own operations and they have an interest in maintaining their own security systems. In such cases, the aircraft operator may elect to carry out the requirements for the SIDA inside the building rather than the airport operator doing so.

Airport operations are able to use existing procedures and resources to cover these new SIDAs and will not need to create different procedures and resources in order to comply with the requirements of this final rule. This approach also ensures that common standards apply on these airports.

In contrast, airports that are not required to have security programs under part 1542 are not required to create SIDAs. At these airports, TSA requires aircraft operators under full all-cargo security programs to prevent unauthorized access to the operational areas of the aircraft, rather than requiring the airports to create SIDAs and corresponding support structures. TSA determined that requiring these airports to create SIDAs would necessitate that they adopt TSA-approved security programs.

TSA declined to extend the scope of these regulatory requirements to entities that currently do not have TSA-approved security programs. TSA determined that requiring aircraft operators to meet the security requirements of § 1544.225 would provide the greatest operational flexibility at airports that do not have TSA-approved security programs.

Many commenters appear to have interpreted the proposed requirements to extend the airport SIDA to cargo operations areas in § 1542.205(a)(2) as applying to off-airport facilities or general aviation areas where cargo may be loaded on or unloaded from smaller all-cargo aircraft. TSA is reiterating the intent of the proposal and clarifying the applicability of this section by modifying the proposed language in the final rule. As stated in the NPRM ''[t]he SIDA would only be extended to areas on airport grounds.'' [12] Part 1542 only applies to airports.

TSA's intent in expanding the SIDA is to deny unauthorized individuals access to the cargo operations areas in order to prevent tampering with the aircraft and cargo and to deny a potential access point for stowaways. TSA believes that expanding the SIDA will minimally affect areas where general aviation aircraft operate. However, TSA acknowledges that each airport is different and some consideration must be given to how SIDA expansion affects general aviation. Each Federal Security Director has authority to work with airport operators to design the SIDA based on local airport characteristics and security requirements.

In response to a question by Juneau International Airport, there is no requirement that SIDAs for cargo operations be contiguous with other SIDAs at the airport. For instance, TSA understands that some airports have SIDAs where passenger operations are conducted that are on the opposite side of the airport from areas where cargo operations are conducted. The area between these locations may not need to be a SIDA.

Comment: UPS recommends that TSA require airports with electronic fingerprint equipment to accept the aircraft operator's and IAC's Submitting Office Number to reduce the costs to the aircraft operator and IAC. UPS states that the Submitting Office Number allows the aircraft operator and indirect air carrier to be billed directly for the CHRC and to identify where the results should be routed. Additionally, UPS states that it is impractical for aircraft operators and indirect air carriers to have electronic fingerprint equipment at all locations for employees that need a CHRC.

TSA response: TSA does not prohibit airport operators from electronically submitting requests for a CHRC by an aircraft operator using that aircraft operator's Submitting Office Number. TSA does not regulate how airports use their equipment in this context. However, IACs are not authorized to conduct CHRCs under this rule.

[12] 69 FR 65270 (Nov. 10, 2004).

II.D. Known Shipper Program

Comment: Several IACs and the National Industrial Transportation League request that TSA clarify issues surrounding accessibility of the proposed known shipper database and recommend the establishment of a central database managed by TSA. In addition, the commenters seek clarification from TSA on how, and to what extent, air carriers' internal systems would be able to interface with the database.

TSA response: TSA agrees, and has developed a centralized database of known shippers.[13] This database is available to the regulated parties. Participating aircraft operators, foreign air carriers, and IACs verify shippers against the database. If the shipper is known in the system, an IAC may offer the cargo for transport to, and the aircraft operator or foreign air carrier may transport their cargo on, a passenger aircraft. The regulated parties may access the system through a web-based portal or by establishing direct access through their air cargo management system.

Comment: A number of commenters believe that the known shipper program should be a TSA-operated function, in order to protect commercially sensitive information. The commenters believe that TSA should establish specific requirements for inclusion in the known shipper list or database, vet shippers for inclusion in the program, populate and maintain the list or database, and make provision for automated verification of shippers against the database.

TSA response: TSA agrees that the operation and management of the known shipper database is a TSA function. However, TSA believes that in order to maintain the carrier's domain awareness and client-vendor relationship, the regulated parties, and not TSA, should perform submissions of known shipper data for inclusion in the database. TSA vets shippers in the database via electronic means. Regulated parties are automatically able to verify shippers against the database through a direct access linkage of their air cargo management system to the known shipper database.

Comment: UPS and FedEx oppose requirements under § 1544.239 to submit known shipper information to a mandatory database. They state that use of the database will diminish rather

[13] This database is covered under the Privacy Act system of records notice. Transportation Security Threat Assessment System (DHS/TSA 002), which was published in the **Federal Register** on September 24, 2004, and amended on December 10, 2004. It can be found at 69 FR 57348, 57349 and at 69 FR 71837.

than enhance security, and question the ability of the TSA database to process the volume of requests and the number of shippers that will be added to the system. In addition, they argue that their competitors could use the database in a manner that would promote unfair competition, and that the servers supporting the database could become inoperable at inopportune times. FedEx states further that the web-based known shipper database will not necessarily be technologically compatible with existing Information Technology (IT) infrastructure and operational demands. UPS wants TSA to treat all information in the database as SSI, and apply stringent privacy protections.

ATA supports the concept of a centralized known shipper database, if the database is secure, transparent to authorized users, accurate, and efficient. ATA states that, at times, the current database is not easily accessible through carrier computer systems and needs a standardized query vehicle, such as a unique identifier for each shipper. ATA states that a mandatory, centralized clearance system raises many questions and challenges for all-cargo carriers not discussed by the ASAC Cargo Working Groups. Therefore, ATA recommends creating a separate task force to examine issues relating to whether all-cargo carriers should participate in the centralized database because of the significant ramifications for the industry. ATA recommends also that TSA fund all carrier costs associated with participation in the known shipper program.

TSA response: TSA believes that the known shipper database will be able to handle the volume of queries. Regulated entities will not be required to have each satellite location equipped with a direct connection to TSA. Rather, these locations may work through a single corporate point of contact.

TSA understands that some operators have expressed concerns that the database may be used in a manner inconsistent with fair competition. TSA notes that regulated entities with access to the database will not be able to produce the entire list of known shippers in a single query. Rather, regulated entities will only be able to confirm a single known shipper at a time. Additionally, TSA notes that it will soon be far less costly for customers to become known shippers with the transition to TSA-vetting. At present, each regulated entity must invest time and effort in making customers known shippers. In the future, TSA will transition this system to allow regulated parties to request that TSA verify that a shipper may be a known shipper. Accordingly, there will be fewer competitiveness issues. TSA remains sensitive to issues of connectivity and competitiveness, and will continue to work with interested stakeholders as we develop these systems.

Currently, the known shipper database employs a verification process to match the information submitted to other publicly available information and for maintaining data integrity. TSA believes that the use of the known shipper database will expedite the process of shipper verification, while providing the Government the necessary tools to vet shippers adequately before the transportation of cargo on a passenger aircraft.

Air carriers will be able to maintain their current systems and practices, such as the manner in which they flag known shippers within their own systems. In addition, TSA believes that the aviation industry benefits from the reduced time it will take to convert a shipper from unknown to known.

TSA disagrees that a centralized database weakens air cargo security. A Government-owned and -managed database that contains all known shippers affords TSA the opportunity to further vet known shippers, evaluate the threat posed by those who use the air transportation system to move goods before the goods are loaded on passenger aircraft and improve efficiency in vetting known shippers. The database treats information that aircraft operators, foreign air carriers, and IACs submit as SSI. TSA will continue to work with regulated parties who have concerns about system continuity and issues of competitiveness as we further develop these systems.

Comment: One commenter proposes merging known shipper and the Automated Export System (AES) databases to avoid redundancy.

TSA response: The AES is a joint venture between Federal agencies and the export trade community. It is the central point through which export shipment data, required by multiple agencies, is filed electronically with CBP, using an electronic interchange.

TSA and CBP are working on the development of TSA's Freight Assessment System. TSA is looking at ways to leverage CBP's systems in order to avoid duplication of effort. TSA will study the feasibility of merging the known shipper database with CBP's AES as part of this effort.

Comment: Several commenters request that TSA clarify the criteria to establish a shipper as a known shipper. Other commenters request that TSA clarify whether the definition will be uniform for all types of freight and that TSA indicate whether it will expand the known shipper program to include small aircraft operators.

TSA response: The specific criteria that TSA uses for the known shipper program are SSI. TSA does not disclose specifics of the criteria in public documents. The shipper itself does not have a need to know the criteria. Rather, aircraft operators, foreign air carriers, and IACs contact the shipper to qualify it as a known shipper. Known shipper program requirements only apply to the transportation of cargo on: (1) A passenger aircraft under a full program; (2) a passenger aircraft operated by a foreign air carrier under § 1546.101(a) or (b); or (3) cargo being transferred to a passenger aircraft operation under these sections. The known shipper requirements do not apply to cargo transported exclusively on all-cargo aircraft.

Comment: The Air Transport Association of Canada proposes reciprocity between TSA and Canadian known shipper databases to avoid duplication of data.

TSA response: TSA and Transport Canada continue to coordinate on this issue. In general, we welcome the opportunity to collaborate with foreign governments in the harmonization of global air-cargo security requirements.

Known Shipper Program and Foreign Air Carriers

Comment: Several commenters, including Nippon Cargo Airlines, question whether TSA requires foreign air carriers to comply with the known shipper program and ask how TSA implements the program with respect to foreign air carriers. The British Embassy asks TSA to clarify whether foreign air carriers are able to accept only cargo from consigners on a TSA-approved list, and requests that TSA confirm that application of the rule is limited to cargo loaded in the United States.

TSA response: Currently, passenger foreign air carriers operating from U.S. airports are subject to the provisions of the Model Security Program (MSP), which requires the adoption of the known shipper program. All cargo loaded on a passenger aircraft at a U.S. airport is subject to this requirement, whether under an aircraft operator or foreign air carrier security program. These requirements are not applicable to cargo loaded outside the United States.

Known Shipper Program and IACs

Comment: TNT USA, an IAC, contends that the regulation is duplicative of existing anti-terrorism

regulations and legislation. The commenter also states that the rule is a barrier to free trade.

TSA response: TSA disagrees. Rather than acting as a barrier to free trade, this rule enhances the capability of aircraft operators, foreign air carriers, and IACs to more efficiently comply with security program requirements. These regulations are not duplicative as they have a different purpose and address a different security threat than those of other U.S. government agencies, like CBP. As stated in the NPRM, CBP and TSA have distinct security missions in securing air cargo. CBP's mission is preventing terrorist and terrorist weapons, including weapons of mass destruction, from entering the United States.[14] TSA, on the other hand, is responsible for securing both U.S. aircraft and foreign flights destined for the United States from destruction or hijacking and, as a result, is primarily concerned with the illicit loading of explosives, incendiaries, or stowaways on board.

Comment: NCBFAA wants TSA to clarify how long it will take to qualify a known shipper and if an IAC can accept cargo from the shipper during the qualification period. NCBFAA states that the known shipper database must be precise in order to avoid delays and confusion over shipper names and asks if known shipper status applies to all office branches of a qualified shipper. Further, NCBFAA asks if the database is the only source of known shipper information, and how TSA notifies IACs of known shipper revocations. Finally, the NCBFAA asks whether air carriers need to consult the database if an IAC already has verified the shipper status and if there is reciprocity for a known shipper under a similar program in another country.

TSA response: Regulated entities must separately list each location for a known shipper. TSA anticipates that the vetting process will take less time than the current process specified in the security programs and is mindful of the competitive commercial environment in which the regulated entities operate. TSA will address other specific process questions about the database in the security programs in order to protect sensitive security information.

[14] Additionally, customs regulations allow for the movement of cargo ''in bond'' from the initial port of arrival to an inland CBP location where it will be released (inspections prior to release are also conducted at these inland locations) into the commerce of the United States. Under the in-bond process, the cargo remains in customs control with requirements as to who may transport it, and where it may be stored (bonded warehouses) until is released by CBP.

Aircraft operators may accept a certification from the IAC that the cargo has been accepted from a known shipper. There is not presently reciprocity to establish a known shipper in the database based upon a determination under a program in another country.

Comment: The Airforwarders Association wants TSA to address the consolidations of IAC operations, where IACs tender shipments to another IAC, in order to achieve efficiency and expedite the shipment of air cargo. They state that the rule does not consider this consolidation as within the known shipper program allowances, even if the shipper is known to the IAC supplying the shipment.

TSA response: TSA agrees and is addressing this issue in the IACSSP amendments, which will be available for IACs to comment on soon after the publication of this final rule.

II.E. Adoption and Implementation of the Security Programs

The following are comments to §§ 1544.101, 1546.101, 1546.103 and 1548.5.

Comment: AOPA does not want TSA to apply security requirements under these sections to on-demand cargo operations, and wants TSA to limit the application of such requirements to scheduled operations. In addition, a domestic air carrier states that terrorists would likely not choose unscheduled airlines for a hostile takeover, or for placement of an explosive device, because of the inability to plan for the location of the planes. The air carrier also wants to limit the regulations to scheduled air cargo transportation.

TSA response: TSA does not believe that distinguishing charter operations as scheduled or unscheduled in this manner would provide for the appropriate level of security. TSA notes that the flight departures of some unscheduled charters are predictable.

Comment: FedEx, Swiss International Air Lines, Air France, and the International Brotherhood of Teamsters recommend adopting one security program for all aircraft operators and foreign air carriers in the industry, without differentiating between weight and type of aircraft or operation.

TSA response: TSA requirements do not prohibit an air carrier from adopting a single security plan for all of its categories of aircraft sizes provided that the plan meets or exceeds the security requirements for each aircraft used in those operations.

TSA recognizes historical patterns of terrorist attacks and a threat-based, risk-managed approach to security. Terrorists have demonstrated the destructive potential of large turbine-powered aircraft with large capacity fuel loads and speeds. Accordingly, a security regime that differentiates between aircraft on the basis of weight is appropriate, regardless of whether a particular aircraft carries passengers or cargo. At the same time, TSA is mindful of the historical link between terrorist operations and passenger aircraft. Therefore, measures that prevent cargo and cargo operations from being used to carry unauthorized explosives, incendiaries, and other destructive substances or items against passenger aircraft must be provided, regardless of aircraft weight. This rationale underscores TSA's security regime and the particular measures that TSA has developed across the spectrum of civil aircraft operations, whether passenger, cargo, or mixed. Requiring the highest level of security for all sizes of aircraft would add a burden for smaller aircraft, which is not warranted by the current threat.

Comment: FedEx states that, in the past, TSA field agents and foreign government officials have incorrectly assumed that the full all-cargo security program is limited or somehow inferior to the passenger aircraft's full program because it did not contain the term ''full program.'' FedEx states that this misunderstanding has resulted in a loss of confidence in their security program, and in some cases, undue scrutiny and delay. ATA CAA, FedEx, and RAA recommend either eliminating the word ''full'' from the names of all security programs or rename the cargo program.

TSA response: TSA notes that the all-cargo program does not require all of the same security measures as the full program that applies to passenger operations. TSA has changed the title to ''full all-cargo program'' in this final rule for the security program required by § 1544.101(h).

Comment: UPS agrees with the creation of this program as long as the Domestic Security Integration Program (DSIP) remains intact and up to date in the final rule. UPS is opposed to adopting any security program other than the DSIP. UPS believes also that bringing the all-cargo industry up to the standard of the DSIP is an effective way to enhance supply chain security.

British Airways asks whether TSA will eliminate or maintain the DSIP after the incorporation of the two programs. British Airways argues that if the DSIP remains, along with the full all-cargo security program, it would give rise to two standards. They oppose this outcome and recommend treating all cargo operations equally.

TSA response: TSA is conforming the existing cargo aircraft operator security programs and the cargo sections of security programs for passenger aircraft operations to the requirements of this final rule. The mandatory program will supersede the DSIP for all-cargo aircraft operators. This new mandatory program will now be referred to as the full all-cargo security program. The DSIP was a program that all-cargo aircraft operators were authorized to adopt voluntarily in order to engage in certain business operations. However, it is important to note that, in addition to adopting a full all-cargo security program, aircraft operators with an MTOW of more than 45,500 kg that transfer cargo to an aircraft operator in passenger service with a full program under §§ 1544.101(a) or 1546.101(a) or (b), must also register with TSA to engage in these transfers. While each full all-cargo program will contain an option to implement the security procedures to transfer cargo to these passenger carrying aircraft, only those aircraft operators that have also registered with TSA to transfer cargo to passenger operations may do so.

TSA recognizes that some aircraft operators under a full all-cargo program are not in the business of transferring cargo to passenger operations. These aircraft operators do not need to register with TSA or carry out the special security procedures, as long as they do not transfer cargo to passenger operations. Each existing DSIP holder, and any additional aircraft operators with an MTOW of more than 45,500 kg in all-cargo operations, must carry out the specific security procedures and register with TSA prior to transferring cargo to passenger operations. Aircraft operators in passenger services under a full program or under § 1546.101(a) or (b) will be required to verify that the aircraft operator with a full all-cargo security program is on an approved list maintained by TSA in order to accept cargo from it.

Comment: AAPA and Singapore Airlines oppose implementation of extraterritorial measures and instead emphasize collaborative discussions to mitigate the terrorist threat without affecting air cargo operations.

TSA response: In this final rule, TSA regulates the civil operations of U.S. aircraft operators, wherever they may operate. The application of the final rule to part 1546 air carriers is generally limited to operations from and within the United States, or to the United States, effective at the last point of departure. In the latter case, compliance with foreign government security requirements that TSA determines are equivalent to U.S. part 1544 requirements generally comply.

Comment: Japan Airlines asks whether §§ 1546.101 and 1546.103 apply to cargo flights making only a technical stop in the United States.

TSA response: Foreign air carriers operating aircraft in all-cargo operations must apply security measures for technical stops in a similar manner as for passenger operations. These security measures are detailed in TSA-approved security programs, related Security Directives, and emergency amendments. The specific security measures are sensitive security information.

Comment: Several commenters, including Singapore Airlines and the British Embassy, want TSA to treat foreign air carriers under part 1546 as equal to domestic aircraft operators under part 1544. In addition, the British Embassy states that many countries' national security program requirements exceed those proposed by TSA, and wants confirmation that, in such cases, these national security programs will be deemed acceptable to TSA.

TSA response: Parts 1544 and 1546 are functionally equivalent. The United States recognizes that part 1546 air carrier operations conducted in accordance with foreign government procedures, and with a similar level of security to U.S. part 1544 operations, generally suffice to meet TSA security requirements. Foreign government procedures may include measures that are at least comparable to what is required of part 1544 operations.

Comment: IATA and Japan Airlines recommend allowing foreign air carriers to submit existing security programs for approval instead of submitting a new program under these rules. In addition, Singapore Airlines and Nippon Cargo Airlines ask if TSA will accept the current All-Cargo International Security Procedures (ACISP).

TSA response: TSA is adjusting security programs such as the Model Security Program (MSP) and ACISP to achieve the security requirements of the final rule. TSA is issuing these security programs to the regulated parties for review and comment sometime on or after publication of the final rule. Foreign air carriers must still submit all such programs to TSA for review and consideration before final approval. The measures of a part 1546 security program that provide a level of security similar to the U.S. part 1544 operations are generally sufficient for operations departing to the United States, satisfy the requirements of the final rule, and are acceptable to TSA. TSA acts through its international air carrier principal security inspector and works with the regulated party to develop measures capable of producing a similar level of security.

Form, Content, and Availability of Security Program

Comment: Singapore Airlines supports § 1546.103 and AAPA wants TSA to provide air carriers with the information about cargo shippers and IAC security programs. Japan Airlines asks if foreign air carriers have flexibility and discretion with respect to fashioning security measures for inclusion in security programs, so long as those measures are acceptable to TSA.

TSA response: TSA considers all security programs SSI and restricts access to applicable regulated entities. Regulated entities may request amendments to their security program following the procedures established in the regulations applicable to their specific operation. Aircraft operators do not have a need to know the contents of an IACSSP.

Comment: NCBFAA recommends creating a frequently asked questions section on the TSA Web site to address issues regarding each new proposed regulation.

TSA response: TSA offers regulated entities security program updates, including information similar to frequently asked questions sections, through secure web-boards. Questions about accessing these web-boards should be directed to a regulated entity's principal TSA contact.

II.F. Costs of IAC Training and Materials

Comment: Several IACs, British Airways, the Airforwarders Association, and Singapore Airlines support § 1548.11 on training and knowledge for individuals with security-related duties. Other IACs, NACA, RACCA, and Brinks, want TSA to clarify what the required training includes. These commenters ask:

- Who is going to pay for the training?
- What training will TSA require?
- Who will provide the training and training materials?
- How often must IACs train the personnel?
- What is the timeframe for accomplishing the training?

FedEx proposes that TSA offer training and certification directly to any trucker or warehouseman who wishes to volunteer, and use vendor certification as evidence of IAC training. In addition, FedEx states that the contractors should directly pay for training, and TSA should pay for the expense of administering the training.

TSA response: TSA is developing computer-based instructional materials and a testing tool, including a minimum standard that an employee must meet and protocols for situations where employees fail to meet the threshold. TSA also is developing the curriculum and training materials, and is including specific requirements for training and testing IAC employees in the revision of the IACSSP. The rule requires that training be completed at least annually for each authorized employee or agent. The IAC bears the cost of training each of their employees or agents.

Comment: FedEx objects to holding IACs responsible for training and testing employees of contractors, subcontractors, or agents, such as truckers or warehousemen, who may have unescorted access to cargo. They believe the proposal is impractical, cost-prohibitive, and that it would impose an unfair burden on IACs. FedEx argues that TSA has underestimated the number of individuals who will require training, as well as the cost associated with the training. FedEx states that TSA calculated only the cost associated with training employees of an IAC, but that it did not include the cost associated with an IAC training the employees of any agents, contractors, or subcontractors that may have unescorted access to air cargo. FedEx interprets this requirement to mean that they would have to train all drivers, warehouse, and office staff of any trucker or courier who may pick up cargo designated for shipping via airfreight. They state further that there are several million licensed drivers in the United States, and even if only 25 percent (approximately 500,000) drivers are involved in the delivery of air cargo, according to TSA's estimate of $100 per individual for the cost of training, the cost to IACs will exceed $50 million. This estimate does not include the cost associated with training new hires, as there is a high turnover employee rate in the trucking industry.

TSA response: TSA has clarified the applicability of IAC requirements. The regulation requirements apply to regulated party employees and agents. If an IAC uses others to perform functions that have security consequences, the IAC must make sure that those persons have proper training. TSA is not requiring air cargo operators with a security program to comply with IAC requirements and believes FedEx has extended its estimate beyond the requirements of this regulation.

II.G. Cost Benefit Analysis

A separate final regulatory analysis is provided on the docket. A summary of the final regulatory analysis appears in this document under the section ''V. Rulemaking Analyses and Notices, A. Regulatory Evaluation Summary.'' To assist the readers of this section, TSA is providing a table that shows, at the summary level, the changes from the NPRM to the final rule. The details of these changes are found in the full regulatory evaluation on the docket. Summary of changes:

Requirement	10 year cost			Remarks
	NPRM	Final rule	Delta	
Costs First Associated With Requirements Under November 2003 SD & March 2005 Security Program Amendments				
Passenger Flight Cargo Screening (first implemented under SD, currently done under security program amendment).	$493.1M	$1,491.1M	+$998.0M	Cost driven by congressional mandate to triple cargo inspections and public comment.
All-Cargo Flight Cargo Screening (currently done under SD).	166.4M	328.0M	+161.6M	Public inputs on costs.
Require All-Cargo operators to screen persons entering aircraft(currently done under SD).	33.7M	35.2M	+1.5M	Implementation cost change.
All-Cargo Security Coordinators (currenlty done under SD).	0.2M	0.0M	−0.2M	Double Counted in NPRM.
Subtotal	693.4M	1,854.5M	1,160.9M	
Costs Associated With Requirements Originating Under This Rule				
Security Threat Assessment	$3.7M	$4.6M	+ $1.0M	Population Increase but admin cost greatly reduced.
Security Identification Display Area (SIDA)	0.9M	10.9M	+10.0M	Costs Identified in comments.
CHRCs for individuals inspecting cargo	0.5M	5.7M	+5.2M	Increased Population.
Implementation of All-Cargo security program for aircraft over 45,000 kg.	26.6M	0.7M	−25.9M	Removed LEO costs.
New aircraft inspection requirements	36.6M	38.2M	+1.6M	Implementation cost change.
TSA Managed Known Shipper Database	24.5M	24.5M	.....	Remained the same.
Develop/implement IAC and Agent Training	15.1M	35.6M	+20.5M	Increase in population requiring training and training development cost.
IAC Security Program Requirements	36.0M	46.5M	+10.5M	Change in Population.
Subtotal	143.9M	166.7M	+22.9M	
Total	837.3M	2,011.9M	+1,183.8M	

Comment: ACI–NA and the Atlanta International Airport believe that airports and IACs should not be obligated to obtain equipment and staff to support these regulations. They believe that TSA or DHS should either fund the new security mandates or take responsibility for securing cargo operations. United Airlines believes that the NPRM's economic analysis fails to consider the impact on U.S. passenger carriers. United Airlines believes the solution is to enact a cargo-screening program based on Federal screening of freight as Congress intended. United Airlines believes that TSA should review methods of defraying costs borne by carriers before they pursue screening initiatives that burden carriers.

TSA response: Only cargo accepted under the known shipper program may

be transported on a passenger aircraft; however, Congress chose not to require Federal Government employees to conduct screening of such cargo. Moreover, Congress did not require that Federal employees must conduct cargo screening for aircraft in all-cargo operations. TSA has required aircraft operators conduct cargo screening since November 2003, and, in part to mitigate the costs cited by the commenter, provides a degree of flexibility for the operators to fulfill these requirements within their operational environment.

Comment: RACCA estimates that because of the high turnover rate in the industry, actual STA cost per employee is $150. RACCA believes that air carriers need this money for applications that have a direct bearing on safety, like pilot training and aircraft maintenance. RACCA states that the threat is minimal, but the cost may be crippling for an industry that operates with narrow margins. They state further that these costs are a burden for many small air cargo operators and may precipitate cost-cutting measures that will have a negative impact on overall safety.

TSA response: RACCA did not provide sufficient information to determine how they computed actual STA costs per employee. TSA has been able to further refine the STA systems and eliminate some costs, lowering the cost of STA per applicant. As our vetting and credentialing capabilities have grown, we are now able to accomplish these checks more expeditiously and economically. TSA allows certain comparable checks in lieu of an STA. Additionally, there is no requirement to renew an STA as long as the STA-holder qualifies as continuously employed. Lastly, in a post 9/11 world, industry must meet both safety and security requirements.

Comment: IATA estimates implementation will be 2 to 4 times higher than the TSA estimate ($3.7 million), or $7.4 to 14.8 million over 10 years. For the expansion of SIDA, IATA estimates that the cost to the industry is 4 times the TSA estimate ($1.4 million), or $5.6 million over 10 years. IATA estimates that the actual cost to implement full all-cargo security programs will be 3 to 4 times the TSA estimate ($26.6 million), or $80 to $106 million over 10 years. Although TSA did not provide any cost estimates for the implementation of the known shipper database, IATA estimates the cost to the industry to be between $1 and $2 million per year. For the enhancements to the IACSSP, IATA estimates that the costs are 25 to 30 percent greater than the TSA estimate ($36 million), or $45.0 to $47.0 million over 10 years. IATA estimates that the training requirements for IACs will be 2 times that TSA estimate ($15.1 million), or $30 million over 10 years. Overall, IATA estimates that the proposed rules will cost the industry 80 percent more than the TSA estimate ($49 million), or $88 million a year.

TSA response: Although the STA population numbers did in fact increase in the final regulatory analysis, there was a corresponding decrease in the unit costs of the STA as TSA was able to eliminate some costs. The new number for the STA is $4.6 million for the 10 years. TSA is providing a reduction in the unit cost of the STA check from $55 to $38, which explains TSA's computed cost of $4.6 million versus IATA's $7.4 to $14.8 million. TSA accepted recommendations from IATA and others, and the SIDA expansion rounds to $10.9 million over 10 years. TSA's recalculation for the IACSSP of $46.5 million is near the top of IATA's $45–47 million. The new IAC training numbers are $35.6 million versus IATA's $30 million. Contrary to IATA's comment that TSA did not provide information on Known Shipper costs, TSA documented those costs as TSA costs rather than industry costs in the NPRM evaluation. A discussion of the Known Shipper program costs are on page 46 of the final regulatory evaluation.

Comment: ATA and British Airways question the distribution of the funding for the proposed rules. They state that, as currently allocated, the costs fall disproportionately on air carriers, because estimated air carrier allocation ($758 million) constitutes 90 percent of the total estimated security costs ($837 million). They state further that the annual costs to all parties will exceed the $100 million annual threshold and would make the NPRM significant under Executive Order 12866.

TSA response: TSA has determined that this rule is significant under Executive Order 12866 guidelines, as discussed in the Regulatory Evaluation Summary of this preamble (Section V.A.). TSA has listened to concerns both about cost and security. The largest portions of costs are directly related to the actual screening conducted by the airlines. TSA believes it has complied with legislative intent that this be a private sector responsibility rather than a governmental function. TSA is unaware of a mechanism for the government to redistribute private sector costs for the required inspections.

Comment: Delta estimates that the financial impact to aircraft operators in year one will be $56.2 million, or $493.1 million in 10 years, and states that the proposed unfunded security mandates add significant costs to their business. Delta believes that TSA's assumptions about aircraft operator's ability to secure operating and capital funding for screening are not correct. Delta believes further that TSA-based calculations from an early 2002 report are significantly inaccurate, and expresses concern about the continued viability of cargo in the passenger air carrier market.

TSA response: TSA computes the ten year impact to the carriers at $1.9 billion versus approximately $760 million in the NPRM evaluation. TSA has accepted numerous inputs from the public comments to revise the cost estimates. The largest portion of these costs, the screening costs, has been in place for sometime, through Security Directives and security program amendments. TSA is codifying these measures at this time. Also, the tripling of cargo screening as required by legislation was the single largest source of change. TSA is not making any assumptions about capital availability to aircraft operators. The fact that the screening requirements have been in place would suggest that the market has already adjusted to a requirement affirmed in legislation. Assumptions about capital expenditures in the full evaluation were based upon the likelihood of future cost savings using automated equipment over manual inspections. The evaluation reiterates that TSA has not mandated the purchase of any screening equipment in this rule. Other than screening equipment, TSA is unaware of what other capital costs Delta might be referencing.

Comment: FedEx states that as proposed, the rules will require STAs for over 500,000 drivers that have potential access to cargo. According to this estimate, STA implementation will cost the industry $27.5 million for only truck drivers ($55 per individual). NACA states that the TSA estimate of employees that will require training is below the actual number, and NACA estimates that in their industry alone, 20,000 people will need the proposed training.

TSA response: The public comments clearly reflected a broader assumption about requirements than TSA intended. TSA has examined the need for STAs in passenger and cargo operations and has reworded the scope of the new requirements more clearly to state which employees and agents of a carrier do require the STA in accordance with security considerations. TSA has adjusted these costs with these new population estimates to reflect TSA's expectation of a narrower coverage than reflected in the public comments.

Comment: NCBFAA states that TSA underestimates the cost of the new measures for air forwarders, many of which are small businesses. NCBFAA questions the basis for TSA's estimate of 3,800 IAC entities and 26,600 IAC employees. NCBFAA questions the lack of underlying support for this conclusion, and believes more employees will be affected by the proposed rules. To support this, NCBFAA states that most IACs are also surface and ocean forwarders, non-vessel operating common carriers, customs brokers, warehousemen, and motor carrier brokers. Hence, the number of employees directly involved in airfreight operations is only a portion of the total employees that might have access to cargo. Consequently, NCBFAA states that the TSA estimate for total compliance ($51 million) is an understatement of the true cost to the industry. NCBFAA recommends TSA undertake a more comprehensive impact and regulatory flexibility analysis of the IAC industry for more accurate assessment of the IAC population.

TSA response: TSA maintains an operational database that reflects approximately 3800 IACs who have identified themselves to TSA. These businesses already interact with TSA security personnel and TSA has identified them as currently providing services to aircraft operators. During preparation of the final rule, the 2002 Economic Census data became available which revealed both more firms and a higher average employee per firm value for the general group of freight forwarders. Public input during the comment period and discussions at TSA revealed that there was a misunderstanding of the STA coverage. Clearer language has been provided and consequentially this evaluation expanded the numbers to use the 2002 Economic Census [15] numbers, which were unavailable at the time of the original evaluation. Please see the separate full regulatory evaluation available on the docket. STAs and the changes are discussed in the section labeled Cost of Compliance: Name Based Background checks and Table 17.

Comment: AAAE believes that the proposed rules are an unfunded mandate for airports. They state further that the cost of expanding SIDA involves more than just the physical expansion of the space; airports with more remote cargo operating locations will need to increase the number of law enforcement personnel on the cargo ramp, while diverting law enforcement resources away from the passenger terminal facility. In addition, AAAE states that airports may need to expand significantly their badging offices to accommodate the additional cargo personnel, and states that the Memphis-Shelby Airport will have to badge 15,000 FedEx personnel.

TSA response: TSA reiterates that not every worker requires a background check, SIDA clearance, and a new badge. The SIDA guidelines have been adjusted to allow the airports to work with aircraft operators to minimize the expansion of the SIDA, while still providing the necessary security. For example, the final evaluation clarifies that additional law enforcement officers do not need to be employed. Rather, the requirement is to have the ability to contact existing law enforcement officials. Also in the full regulatory evaluation, section on ''Cost of Compliance: Airport Operators,'' TSA has shown how it used the public comments to revise the costs and population needing badges. Based upon the information in comments, TSA believes it reasonable to reject the need to increase staffing for this expected one time increase. Memphis is an example of several locations that have national hubs for the Nation's largest parcel and express shippers. TSA invites the airport and shippers to work with us in order to use the flexibility and alternatives that TSA authorizes.

Comment: IATA states that TSA underestimates the number of affected employees, and two IATA members indicate that depending on the definition of unescorted access to cargo, they will have at least 63,000 impacted staff, mainly cargo handlers and drivers. The Airforwarders Association states that TSA's estimate of the number of IACs is correct, but that the number of affected IAC employees is incorrect, and recommends revaluation. ATA states that depending on the scope of the requirement, the number of individuals subject to either an STA or CHRC could be ten times greater than the 63,000 estimated by TSA.

TSA response: TSA has examined the public comments along with new data available in the 2002 Economic Census.[16] Census numbers do not support a three-fold expansion of the population while keeping the number of businesses constant. The new Census number of firms and the average employee per business value increased only slightly. Additionally, given that some of the public comments agree with TSA's original numbers, TSA believes that there has been confusion on to the extent the STA or CHRC were going to be required. The full regulatory evaluation provides several pages of detail in the section ''Cost of Compliance: Indirect Air Carriers'' and in the full evaluation tables 13–17. Based on extensive internal discussion of very knowledgeable subject matter experts, TSA believes the new language provides much clearer guidance and the Census number adjustments are an appropriate estimate.

II.H. 100 Percent Inspection of Cargo

TSA invited comments in the NPRM, but did not propose requirements, for the physical inspection of 100 percent of air cargo.

Comment: The majority of comments TSA received on this issue, including comments from Air France, ATA, British Airways, IATA, Singapore Airlines, and several IACs, oppose 100 percent inspection of air cargo. The consensus of these comments is that requiring 100 percent inspection of air cargo would be impractical in an industry dependent on just-in-time deliveries, without advances in targeting methodology, data, and technology. ATA states further that the 100 percent inspection of cargo is not warranted or required under ATSA, nor is it justified under any risk-based analysis that TSA has shared with the industry. A small minority of comments, including comments from ALPA and the International Brotherhood of Teamsters, support 100 percent inspection of air cargo.

TSA response: TSA is not requiring 100 percent inspection of air cargo at this time. As mentioned in the proposal at 69 FR 65266, TSA considered requiring 100 percent inspection of air cargo, but determined to continue with a layered approach of security measures and to pursue a risk-based targeting strategy to identify higher risk cargo for additional scrutiny. This conclusion is affirmed by, and derived from, the Government Accountability Office report on Vulnerabilities and Potential Improvements for the Air Cargo System,[17] the Department of Transportation's Office of the Inspector General Audit of the Cargo Security Program,[18] and TSA's Air Cargo

[15] 2002 Economic Census, Support Activities for Transportation: 2002, Transportation and Warehousing Industry Series at *http://www.census.gov/econ/census02/guide/INDRPT48.HTM.*

[16] Support Activities for Transportation: 2002, Transportation and Warehousing Industry Series at *http://www.census.gov/econ/census02/guide/INDRPT48.HTM.*

[17] GAO–03–344, December 2002.

[18] Report Number SC–2002–113, Sep. 19, 2002. This report is SSI.

Security Scenario Analysis. These reports have cautioned that, in the absence of an appropriate targeting methodology and data, requiring inspection of 100 percent of air cargo would severely burden the just-in-time delivery that is currently a key competitive feature of many U.S. manufacturing and distribution industries. In addition, 100 percent inspection could have particularly severe negative impacts on aircraft operators, IACs, and their employees and agents. TSA has focused on deploying currently available tools, resources, and infrastructure in a targeted manner to provide effective security in the air cargo environment, and has laid out a path for accelerated research and development of even more effective tools.

II.I. Unknown Shipper Cargo

TSA invited comments in the NPRM, but did not propose requirements, about allowing unknown shipper cargo on passenger aircraft after proper screening.

Comment: ATA, CAA, Delta, RAA, and other commenters request that TSA consider allowing cargo from unknown shippers into passenger aircraft after proper screening. These comments assert that TSA should permit cargo on passenger carriers subject to inspection.

TSA response: While TSA appreciates these comments, at this time TSA declines to allow the transport of unknown shipper cargo on passenger aircraft. Currently, no technology or inspection techniques exist with sufficient versatility to handle the vast array of cargo configurations, and commodities to ensure security, while maintaining acceptable throughput, or processing time. TSA continues to collaborate with the industry in an effort to develop technology solutions to improve the effectiveness and efficiency of the cargo screening process.

II.J. Terms Used in This Subchapter

Comment: British Airways, AEA, IATA, and the International Brotherhood of Teamsters support the definition of ''Indirect air carrier'' in § 1540.5. British Airways and AEA state that the expanded coverage is consistent with proposals from the European Commission. AAPA and IATA suggest that the definition should include equivalent entities of IACs operating outside of the United States. Purolator suggests that the United States Postal Service and foreign postal services should be included in the definition.

TSA response: TSA is working closely with the European Commission to establish the basis of mutual recognition of its regulated agent and/or IACSSP. The U.S. Postal Service is not subject to the provisions of this rule. The security of the U.S. Mail is covered under a Mail Security Program that provides an appropriate level of security for mail transported via aircraft.

Comment: The Denver International Airport wants TSA to define the term airport grounds, and three commenters recommend adopting a definition for the terms ''cargo'' and ''access to air cargo.''

TSA response: ''Cargo'' is defined in 49 CFR 1540.5. TSA is revising the language of §§ 1544.228, 1546.213, and 1548.15 to include those individuals specifically authorized by the aircraft operator, foreign air carrier, or IAC to have unescorted access to air cargo. As stated in the preamble to the NPRM at 69 FR 65270, ''The SIDA would only be extended to areas on airport grounds.'' The requirement to extend SIDA to cargo operations is specific to the area used by an aircraft operator under a full all-cargo program, as provided in § 1544.104(h) and by a foreign air carrier under § 1546.101(e). Therefore, the proposed extension of the SIDA applies only to those areas regularly used to load or unload cargo on larger all-cargo aircraft under a full all-cargo security program. TSA is modifying § 1542.205(a)(2) to reflect this intention by adding the words ''air operations area'' instead of the words ''airport grounds'' and by deleting the reference to areas used ''to sort cargo.''

Comment: Air France and Global Express Association propose that TSA harmonize terms used in cargo operations, like ''known shipper,'' ''consignor,'' ''regulated agent,'' and ''IAC.''

TSA response: TSA believes that the terms ''known consignor'' and ''known shipper'' are similar, in general. However, TSA's use of the term ''known shipper'' is specifically dependent on meeting the criteria and required measures in TSA-approved security programs. Similarly, the terms ''regulated agent'' and ''indirect air carrier'' are alike, in general. However, TSA's use of the term ''indirect air carrier'' only applies to entities within the United States, and subject to the required measures in TSA-approved security programs, while ''regulated agents'' are located outside of the United States and subject to ICAO standards and a State's national requirements.

II.K. Persons and Property Aboard the Aircraft

Comment: CAA, FedEx, NACA, and UPS recommend that TSA revise §§ 1544.202 and 1546.202 to apply only to persons who board the aircraft for transportation. ATA recommends distinguishing individuals and the applicable screening requirements to require 100 percent screening of individuals boarding the aircraft for the purpose of transportation, and random screening of those boarding the aircraft for a limited purpose and amount of time.

TSA response: TSA is adding the phrase ''for transportation'' in §§ 1544.202 and 1546.202. The intent of proposed §§ 1544.202 and 1546.202 is to screen persons who are onboard the aircraft in flight, for weapons, explosives, incendiaries, and other destructive substances or items. Persons who enter the aircraft on the ground for servicing or maintenance are subject to other security measures, which may include some screening for prohibited items, in airport areas where all-cargo aircraft operations are conducted.

II.L. Other Issues and Sections

Proposed Compliance Schedule

Comment: AAAE, the Savannah Airport Commission, the NCBFAA, and others state that the compliance schedules are brief and unrealistic. AAAE recommends providing waivers to airports that cannot comply in 90 days. Only one commenter, an insurance company, states that the 180-day schedule to introduce new training requirements is too long.

TSA response: TSA believes this final rule allows adequate time for airport operators, aircraft operators, foreign air carriers, and IACs to comply. Further, TSA notes that the complexities involved in compliance, as well as anticipated costs, have been carefully weighed where deadlines are established. Where difficulties are encountered, airport operators, aircraft operators, foreign air carriers, and IACs are encouraged to contact their TSA Principal Security Inspector or local Federal Security Director. TSA attempts to ensure a realistic approach to compliance timeframes, but recognizes that such timeframes are sometimes not met for good cause, and is prepared to extend reasonable consideration on a case-by-case basis, as warranted.

Use of Loring Air Force Base

Comment: Ten commenters, including the U.S. Senate Committee on Government Affairs, a U.S. Representative from Maine and the Governor of Maine, recommend the use of Loring Air Force Base in Northern Maine as an emergency site to land inbound international cargo aircraft found to pose an imminent threat.

TSA response: The Intelligence Reform and Terrorism Prevention Act of 2004 requires the Secretary of Homeland Security, in coordination with U.S. Department of Defense and FAA, to submit a report on current procedures to address the threat of all-cargo aircraft that are inbound to the United States from outside the United States, and an analysis of the benefits of establishing secure facilities along established aviation routes for the purposes of diverting and securing aircraft that may pose a threat. While this rule does not specifically address this issue, TSA is considering these comments in the development of the report to Congress on the feasibility of establishing these sites as required by sec. 4054 of the Intelligence Reform and Terrorism Prevention Act of 2004.

STA for Passengers of All-Cargo Aircraft

TSA invited comments in the NPRM, but did not propose requirements, about requiring each person who boards an aircraft for transportation under an all-cargo security program to submit to an STA. TSA also invited comments about requiring persons who board an aircraft under an all-cargo security program who require prohibited items during the flight to perform their duties to submit to the assessment. There are five comments on this issue.

Comment: Three commenters, British Airways, Air France, and ALPA, support STAs for individuals who board all-cargo aircraft for transportation. ALPA states that TSA must minimize access to the aircraft and the flight deck by permitting only those persons to board who have been properly vetted by a 10-year, fingerprint-based CHRC. They also state that TSA should reconsider the practice of allowing employees who have not been vetted to ride aboard all-cargo aircraft as an employment benefit, without requiring them to meet the same security requirements applicable to other employees who work on or around the aircraft. In addition, ALPA notes that many foreign nationals travel as animal attendants aboard all-cargo aircraft, and often sit unsupervised just outside of the cockpit, in possession of items normally prohibited on aircraft.

Two commenters, ATA and IATA, oppose this requirement. IATA states that STAs for personnel boarding all-cargo aircraft are unnecessary when the Government has already vetted such personnel through the submission of master crew lists and flight manifests. Similarly, ATA recommends permitting air carriers to use current comparable procedures in these locations like submission of crew manifests to TSA.

TSA response: TSA appreciates the responses to this particular issue and is further evaluating the impact and benefit of establishing an STA requirement for individuals onboard an all-cargo aircraft. At this time, TSA declines to extend an STA requirement to these individuals. Screening requirements for individuals transported are addressed in applicable security programs, Security Directives, and Emergency Amendments. Individuals transported are currently checked against the TSA ''No Fly'' list and their persons and accessible property are inspected for prohibited items.

Security of Aircraft and Facilities

Comment: UPS recommends further clarification of ''operational area of the aircraft'' in § 1544.225(d) and suggests alternative regulatory text. The Airports Consultants Council asks if this provision transfers the responsibility for airport access control for an Exclusive Use Area and states that, if it does, TSA should clarify.

TSA response: TSA declines to amend § 1544.225(d). TSA is providing more clarification to this section through the security program revision. This provision does not transfer the responsibility for airport access control for Exclusive Use Areas. Under §§ 1542.111 and 1544.227, airports and aircraft operators may agree that control over a SIDA at cargo operations can be transferred to an aircraft operator.

Fingerprint-Based CHRCs: Unescorted Access Authority, Authority To Perform Screening Functions, and Authority To Perform Checked Baggage or Cargo Functions

Comment: Four commenters, including ATA and ALPA, support § 1544.229. Swiss International Airlines notes that fingerprinting may not be necessary for an effective background check, and suggests that TSA harmonize these requirements with existing EU regulations.

TSA response: TSA continues to collaborate with its foreign counterparts, where possible, in harmonizing security measures.

IAC Security Programs: Approval, Amendment, Annual Renewal, and Withdrawal of Approval

Comment: While the majority of commenters support § 1548.7, some believe that the process requires applicants to submit information already held by DHS under CBP's Customs-Trade Partnership Against Terrorism program. The Airforwarders Association asks if § 1548.7(a)(1)(v) requires only addresses for United States and not foreign locations. In addition, the Airforwarders Association recommends facilitating the requirements of § 1548.7(a)(5) through harmonization of a non-governmental organization accreditation program. ACC opposes the duration of the § 1548.7(a)(4) security program, and proposes instead that TSA grant only one initial approval, subject to continued inspection, to avoid processing of thousands of security programs each year.

TSA response: TSA currently is evaluating the synergies that may exist between TSA's IAC and CBP's Customs-Trade Partnership Against Terrorism programs, and would consider changes to the IACSSP if appropriate. Part 1548 does not apply to stations or locations outside the United States. TSA believes that the yearly revalidation process assists the IAC in reviewing its security posture and compliance with TSA requirements. Furthermore, TSA believes that a yearly revalidation requirement does not impose an unreasonable burden on the IAC community.

IAC Security Coordinators

Comment: Singapore Airlines, British Airways, ACC, and others support § 1548.13. ACC, ACI–NA, and the Atlanta International Airport ask if this requirement is similar to aircraft operator security coordinator requirements and ask if aircraft operators must update their security programs to include IAC security information.

TSA response: This requirement is based on the model of requirements for aircraft operator security coordinators. TSA does not require aircraft operators, foreign air carriers, or airport operators to maintain records of IAC security coordinators as part of their security programs.

Comment: Freight Forwarders International questions the purpose of the security coordinator and what specific information TSA requires from this person.

TSA response: The purpose of the security coordinator is to act as the security liaison between the regulated party and TSA. The security coordinator provides a single point of contact for communications involving threat information or security procedures, particularly those that are time-sensitive in nature. TSA is revising the IACSSP to include specific requirements for security coordinators.

Comment: NCBFAA believes that the security coordinator requirement is impractical and unworkable for many

IACs, and imposes a particularly unnecessary burden upon smaller companies. As an alternative, NCBFAA recommends permitting an IAC to contract with a third party to act as its security coordinator or to rely on a contact person who works with the air carrier.

TSA response: TSA believes that IAC personnel must perform the functions of the Security Coordinator. It is crucial that the security coordinator be in a position to identify security problems, raise issues with corporate leadership, and initiate corrective action when needed. The security coordinator and alternates must be appointed at the corporate level, and must serve as the IAC's primary contact for security-related activities and communications with TSA. Furthermore, TSA believes that having a single person responsible better assists the IAC to meet current IAC requirements for oversight of the actions of agents performing security functions on behalf of the IAC.

Security Directives and Information Circulars for IACs

Comment: Many commenters support § 1548.19, and IBM recommends making a sanitized Information Circular available to the shipping public, in particular if there is need for additional screening or inspections.

TSA response: In principle, TSA agrees that there must be wide-ranging public access to security information, particularly as needed for compliance with security requirements and procedures. However, information that, singly or collectively, might indicate intelligence sources, methods or procedures, or aviation security procedures, must be protected. Striking the balance between these principles generally requires that access to particular pieces of security information be considered on a case-by-case basis.

III. Section-by-Section Analysis of Changes

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

Section 1520.5 Sensitive Security Information

TSA provides the conforming amendments to § 1520.5(b) consistent with our proposals to restrict this information from public dissemination. TSA now expressly includes as SSI Security Directives and Information Circulars for IACs.

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

Section 1540.5 Terms Used in This Subchapter

TSA is amending the definition of ''Indirect Air Carrier'' to conform to other changes pursuant to this final rule. With these changes, freight forwarders who offer cargo to operators of larger all-cargo aircraft must have a TSA-approved security program. Accordingly, TSA has modified the definition of ''Indirect Air Carrier'' by removing the word ''passenger'' from ''uses for all or any part of such transportation the services of a passenger air carrier'' in order to be consistent with TSA's goal of extending a security regime to full all-cargo aircraft operations.

TSA has also provided a definition for ''unescorted access to cargo.''

Section 1540.111 Carriage of Weapons, Explosives, and Incendiaries by Individuals

TSA has expanded the applicability of this section to include persons on all-cargo aircraft. TSA amended paragraph (a)(1) by qualifying the applicability of this provision to the entire subchapter (Subchapter C—Civil Aviation Security) rather than to specific sections. This amendment is consistent with the expansion of security functions to persons and property onboard all-cargo aircraft under § 1544.202.

Sections 1540.201 Through 1540.209 Subpart C—Security Threat Assessments

This subpart sets out the scope and basic requirements of a Security Threat Assessment (STA), including related fees. The STA includes a search by TSA of domestic and international databases to determine the existence of indicators of potential terrorist threats that meet the standards set in subpart C of part 1540. The section also provides for review of a TSA determination that an individual should be denied unescorted access to cargo.

Operators are required to ensure that employees and agents whom they authorize to have unescorted access to cargo undergo Security Threat Assessments or other TSA-approved checks under §§ 1544.228, 1546.312, and 1548.15. For a further discussion of the scope for each of these sections, see the section-by-section analysis of § 1544.228 below.

Under § 1540.203 operators are required to verify the identity of the employee or agent and submit specified information about that individual to TSA. TSA has provided a modest amendment to the information each individual must submit under § 1540.203. This amendment includes decreases in the information required on previous residential addresses from seven to five years and adds a requirement to list the gender of the individual. TSA has determined that these changes provide sufficient information to conduct a thorough Security Threat Assessment. After assessing this data to determine whether the individual poses or is suspected of posing a threat to national security, to transportation security or of terrorism, under § 1540.205, TSA would notify the regulated party and the individual of its determination. This determination can take three forms:

1. *Determination of No Security Threat.* This determination indicates that TSA has not found that the individual presents a known or suspected threat to security. Upon receipt of this notification, the operator may authorize the individual unescorted access to air cargo.

2. *Initial Determination of Threat Assessment.* TSA issues this determination if TSA knows or suspects the individual of posing a security threat. The individual is able to appeal this determination through adjudication. Individuals are not permitted unescorted access to air cargo while the appeal is pending. For each proprietor, general partner, officer, director and owner of the entity as identified in § 1548.16, issuance of an Initial Determination of Threat Assessment may delay TSA approval of authority to operate under an IACSSP.

3. *Final Determination of Threat Assessment.* If the individual was determined to present a threat after an initial determination was issued and the individual has an opportunity to appeal that determination, this determination informs the operator and the individual that he or she is barred from having unescorted access to air cargo. For each proprietor, general partner, officer, director, and each owner of the entity as identified in § 1548.16, issuance of a Final Determination of Threat Assessment may prevent TSA approval of authority to operate under an IACSSP. On a case-by-case basis, TSA may withhold authorization of an IACSSP until the IAC, or an applicant to be an IAC, demonstrates to TSA that a proprietor, partner, officer, director, or owner under § 1548.16 who received a Final Determination of Threat Assessment is unable to influence business practices of the IAC.

Section 1540.207 sets out the appeals procedures to provide appropriate due process to individuals determined to

pose a security threat under this subsection, including a written request for materials, within 30 days of receipt of the Initial Determination of Threat Assessment from TSA. TSA has included a cross reference to § 1540.207 in § 1540.205(c)(4). Throughout the STA adjudication process, TSA may consult with other Federal law enforcement or intelligence agencies in assessing whether an individual poses a security threat under this subsection.

Section 1540.209 establishes the fee requirements necessary to recover associated costs for Security Threat Assessments. TSA has modified the sum of the fee from the NPRM to reflect the most recent calculations, as described in the regulatory evaluation.

The operator must not permit employees or agents to handle cargo, until TSA notifies the operator and the individuals of a Determination of No Security Threat. In cases where TSA issues a Determination of Threat Assessment, TSA may notify Government agencies for law enforcement or security purposes, or in the interests of national security. TSA recognizes that the requirement for security threat assessments under this final rule may cause affected businesses to alter their hiring practices. However, TSA believes that the security benefits of this requirement will be considerable and that TSA will be able to conduct the initial assessments in an expeditious fashion, providing timely notice to the regulated party.

PART 1542—AIRPORT SECURITY

Section 1542.1 Applicability of This Part

Part 1542 currently applies to certain airports that serve certain passenger aircraft operations identified in parts 1544 and 1546. These airports are required to have security programs. Some airports are not required to have security programs even though the aircraft operators served by the airport hold security programs under parts 1544 or 1546. These aircraft operators include operations of a twelve-five program under § 1544.101(d) and of a full all-cargo program under § 1544.101(h).

The new § 1542.1(d) expands the applicability of part 1542 to include each airport that does not have a part 1542 security program that serves an aircraft operator with a security program under part 1544, or a foreign air carrier under part 1546. This addition makes clear that TSA may enter an airport to inspect aircraft operators and foreign air carriers even if they are using an airport that is not otherwise required to operate under a TSA-approved security program. It is critical that TSA have access to those aircraft operations to conduct its inspection functions under § 1542.5(e) to determine whether they are in compliance with applicable security requirements.

Section 1542.5 Inspection Authority

TSA added § 1542.5(e) to clarify that TSA may enter and be present at an airport that is not otherwise required to have a TSA-approved security program under part 1542 in order to inspect a TSA-regulated aircraft operator or foreign air carrier.

Section 1542.101 General Requirements

TSA deletes ''under this part'' from the sentence ''No person may operate an airport subject to this part unless it adopts and carries out a security program'' in § 1542.101(a), and adds ''subject to § 1542.103'' to further clarify that airports under § 1542.1(d) are not required to meet other requirements of this part. TSA revises § 1542.101(b) by deleting ''The airport'' and adding ''Each airport subject to ''§ 1542.103'', and § 1542.101(c) by adding ''subject to § 1542.103'' after ''Each airport operator'' for the same reason.

Section 1542.205 Security of the Security Identification Display Area (SIDA)

TSA has clarified the applicability of this section in this final rule by modifying the language that was proposed in the NPRM for § 1542.205(a)(2) to now include the phrase ''the air operations area'' in the section, and has deleted the reference to areas used ''to sort cargo,'' and added new paragraphs (a)(3) and (a)(4). Airports are required to create new, or expand existing, SIDAs to encompass areas on airport grounds where cargo is regularly loaded on, or unloaded from, an aircraft operated under a full program or a full all-cargo program, or foreign air carriers under a security program as provided in § 1546.101(a), (b), or (e). Additionally, TSA clarified the scope of this requirement by adding that the SIDA must be extended on an airport to areas where an aircraft operator, foreign air carrier, or indirect air carrier accepts cargo. Acceptance in this context means taking physical control of the cargo from persons such as a shipper, aircraft operator, foreign air carrier, indirect air carrier, or their respective employees or agents. In particular, this includes inside buildings such as cargo facilities, loading and unloading vehicle docks, and other areas where an aircraft operator, foreign air carrier, or indirect air carrier sorts, stores, stages, consolidates, processes, screens, or transfers cargo.

TSA also revised § 1542.205(b)(2), which stated that an individual must undergo an employment history verification under § 1542.209 before gaining unescorted access to a SIDA. This section requires individuals to complete a fingerprint-based criminal history records check pursuant to § 1542.209, rather than an employment history verification, and is consistent with § 1542.209. Finally, TSA adds § 1542.205(c) to clarify that an airport operator that is not required to have a complete program under § 1542.103(a), is not required to establish a SIDA under § 1542.205.

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

Section 1544.3 Inspection Authority

This section currently refers to TSA inspection authority in secure areas, AOAs, and SIDAs. TSA amended this section under this final rule also to reflect authority to inspect other areas operated by an aircraft operator where it carries out security measures. These areas may include areas off of the airport, or operated by its agent in furtherance of the aircraft operator's security responsibilities. The amended § 1544.3(c) clarifies that TSA may enter and be present where an aircraft operator carries out security measures without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

Section 1544.101 Adoption and Implementation

Under this final rule, all-cargo aircraft operations conducted in aircraft with a maximum certificated take-off weight of more than 45,500 kg (100,309.3 lbs.) must meet security requirements for a full all-cargo program under § 1544.101(h) and (i). TSA refers to these security measures as the ''full all-cargo security program.'' Operations under a full all-cargo security program are no longer authorized to operate under the current twelve-five program, as provided in § 1544.101(d)(1), or under a voluntary domestic security integration program (DSIP).

TSA revised § 1544.101(e)(1), which lists the elements of the twelve-five program in all-cargo operations, to include: § 1544.202 (Persons and property onboard the all-cargo aircraft) and § 1544.205(a), (b), (d), and (f) (Acceptance and screening of cargo:

Preventing or deterring the carriage of any explosive or incendiary, Screening and inspection of cargo, Refusal to transport, and Acceptance and screening of cargo outside the United States).

This section also amends the requirements for aircraft under a twelve-five program from a maximum certificated takeoff weight ''of 12,500 pounds or more'' to ''more than 12,500 pounds'' as authorized under the Century of Aviation Reauthorization Act.[19]

Section 1544.202 Persons and Property Onboard the All-Cargo Aircraft

Section 1544.202 requires aircraft operators to apply security measures to persons who board their aircraft for transportation, and to the property of those persons. The words ''who are carried aboard the aircraft'' are added in place of ''board the aircraft'' to provide clarification of the scope of covered persons. This technical correction is consistent with the language of FAA requirements regarding carriage of persons under 14 CFR 121.583. Section 1544.202 provides the means to prevent persons, who may pose a security threat from boarding, and to prevent or deter the carriage of unauthorized explosives, incendiaries, and other destructive substances or items. This section also provides for TSA to incorporate into security programs screening for unauthorized persons, or substances or items that could be used to pose a threat to transportation security. These requirements apply to both the twelve-five program in all-cargo operations and the new full all-cargo security program.

Section 1544.205 Acceptance and Screening of Cargo

TSA requires aircraft operators operating under a full, full all-cargo, or twelve-five program to prevent or deter the carriage of, and screen and inspect cargo for, any unauthorized persons, and any unauthorized explosives, incendiaries, and other destructive substances or items. This amendment is necessary to prevent and deter the introduction of stowaway hijackers, explosive devices, or other threats into air cargo.

Section 1544.205(c) requires aircraft operators to prevent unauthorized access by persons other than an aircraft operator employee or agent, and adds that persons authorized by the airport operator or host government also may have access. For example, individuals such as customs inspectors and airport law enforcement officers must have access to such areas. TSA revised paragraph (c)(1) by adding ''any unauthorized person, and any unauthorized explosive, incendiary, or other destructive substance or item'' in place of ''unauthorized explosive or incendiary'' to be consistent with the requirement throughout this rulemaking and the identified critical risks.

TSA also strengthened the cargo acceptance requirements applicable to aircraft operators operating under a full program or a full all-cargo program. Pursuant to § 1544.205(e), an aircraft operator may accept cargo for air transportation only from entities that have comparable security programs. TSA will provide more information on comparable programs within the standard security programs. These requirements parallel those currently applied to operations conducted under a full passenger security program, in which the aircraft operator may only accept cargo from another aircraft operator or foreign air carrier with a comparable security program.

TSA also requires each aircraft operator to carry out the requirements of its security program, for cargo to be loaded on its aircraft outside the United States under § 1544.205(f). TSA recognizes that not all the requirements of part 1544 can be carried out in other countries. Accordingly, we work with the host governments, under international agreements, to ensure that the security measures in place provide the appropriate level of security.

Section 1544.217 Law Enforcement Personnel

TSA is providing clarifying amendments to paragraphs (a) and (b), to add missing cross-references. Currently, operations under twelve-five programs and under private charter programs must comply with § 1544.217, regarding arranging for law enforcement support at airports where they operate. See § 1544.101(b), (c), (d), and (e). Requirements for law enforcement personnel are already a part of the security programs for the twelve-five and private charter programs. However, § 1544.217 does not currently refer to those operators. This clarification adds these cross references, as well as adding a cross reference to the new full all-cargo program under § 1544.101(h) and (i).

Section 1544.225 Security of Aircraft and Facilities

New § 1544.225 is amended to add paragraph (d), which requires operators of aircraft operating under a full program or a full all-cargo security program to prevent unauthorized access to the operational area of the aircraft while loading or unloading cargo. This requirement applies to operations conducted both within and outside a SIDA. TSA recognizes that current paragraph (b) requires all aircraft operators operating under security programs to prevent unauthorized access to each aircraft. The revisions to this section broaden this requirement for aircraft operated under a full or a full all-cargo security program, clarifying that the aircraft operator must prevent unauthorized access to the operational area around the aircraft during cargo loading and unloading operations.

Section 1544.228 Security Threat Assessments for Cargo Personnel in the United States

In this final rule, TSA has provided revisions to each section about a regulated entity's responsibilities for STAs. While these revisions comport with the scope of the NPRM, we have restructured the sections significantly, in order to be responsive to comments and provide greater clarity on the scope of personnel who are required to meet the STA requirements. The revisions clarify that the requirements apply to employees and agents of aircraft operators operating under a full program pursuant to § 1544.101(a) or a full all-cargo program pursuant to § 1544.101(h), who are authorized to perform certain security duties without an escort. Likewise, these requirements apply to employees and agents of foreign air carriers under §§ 1546.101(a), (b), or (e), and IACs.[20] Please refer back to the previous TSA responses regarding security threat assessments under section II. Comment Disposition, for more information on this topic.

This section is also satisfied by completion of a CHRC for unescorted access to SIDA, or by another STA approved by TSA. For instance, if the employee or agent has an STA for the issuance of a hazardous materials endorsement on a commercial driver's license, in accordance with § 1572.5, TSA would approve that as acceptable for compliance with § 1544.228.

[19] Vision 100—Century of Aviation Reauthorization Act, Sec. 606 (Pub. L. 108–176, 117 Stat. 2490, 2568, Dec. 12, 2003).

[20] The STA requirements also extend to an officer, director, and person who holds 25 percent or more of total outstanding voting stock of an IAC. However, TSA did not receive requests for clarification to this requirement.

Section 1544.229 Fingerprint-Based Criminal History Records Checks (CHRC): Unescorted Access Authority, Authority To Perform Screening Functions, and Authority To Perform Checked Baggage or Cargo Functions

In the case of passenger aircraft operated under a full program, TSA already requires cargo screeners and their immediate supervisors in the United States to meet the CHRC requirements under § 1544.229(a)(3)(i). This amendments requires that individuals and their immediate supervisors in the United States who screen cargo to be transported on an all-cargo aircraft with a full all-cargo program under § 1544.101(h) submit to a CHRC under § 1544.229.

As stated earlier, TSA already requires airport operators to send to TSA certain personal information for each individual who has undergone a CHRC for a current SIDA or sterile area ID in order to perform an additional background check that is comparable to an STA. TSA is providing instruction to aircraft operators with a full or full-all-cargo security program to send to TSA the same type of information for cargo screeners who do not have current SIDA or sterile area IDs, and will also perform the additional check on this population. Most of these cargo screeners already have SIDA IDs and, thus, already are checked.

Section 1544.239 Known Shipper Program

Section 1544.239 codifies the known shipper program in the Federal regulations. The ''known shipper'' concept, which differentiates cargo being shipped by recognized entities from that originating with unknown parties, has been a fundamental element of air cargo security since 1976. The program has also been recognized as a global standard by the International Air Transport Association (IATA) and was recognized by the U.S. Congress as a form of screening in the ATSA.[21] Passenger aircraft operators operating under a full program are required to have a known shipper program, including measures to ensure the shippers' validity and integrity, to inspect or further screen cargo, and to provide shipper data to TSA. Aircraft operators must meet these requirements in accordance with the standards detailed in their security program. The known shipper program applies to passenger operations under full programs, and to those operations that elect to have a comparable security program that allows interlining cargo to operations under a full program.

[21] 49 U.S.C. 44901(a).

PART 1546—FOREIGN AIR CARRIER SECURITY

Section 1546.3 TSA Inspection Authority

TSA is adding paragraph (c) relating to TSA authority to enter and be present in certain areas in order to inspect or test compliance or perform other duties. This amendment is parallel to the provisions in § 1544.3(c). This amendment reflects TSA's authority in the specified areas.

Section 1546.101 Adoption and Implementation

Cargo operations of foreign air carriers that land or takeoff in the United States are required to conform to essentially the same requirements as those applicable to comparable operations by U.S. aircraft operators. This section broadens the provisions of § 1546.101 to require each foreign air carrier, landing or taking off in the United States, to adopt and carry out an appropriate security program for each covered all-cargo operation. This section establishes the requirements of an appropriate security program for a covered foreign air carrier conducting all-cargo operations in aircraft having a maximum certificated take-off weight greater than 45,500 kg (100,309.3 pounds) (analogous to a U.S. full all-cargo security program under part 1544), and in aircraft having a maximum certificated take-off weight greater than 12,500 pounds but not more than 45,500 kg (100,309.3 pounds) (analogous to a U.S. twelve-five program in all-cargo operations under part 1544). The requirement that a foreign air carrier with operations in aircraft that have a maximum certificated take-off weight greater than 12,500 pounds but not more than 45,500 kg under § 1546.101(f) will supersede the current All-Cargo International Security Procedures requirements under § 1550.7. See 69 FR 3939, Jan. 27, 2004.

Section 1546.103 Form, Content, and Availability of Security Program

In this section, TSA makes an administrative change to paragraph (a), removing the word ''passenger'' and changing ''U.S. air carriers'' to ''U.S. aircraft operators'' to acknowledge that certain all-cargo operations by a foreign air carrier now must be under a security program.

In paragraph (b), TSA adds references to paragraphs (e) and (f) to the introductory text. This change broadens this section's requirements to encompass cargo operations.

Section 1546.202 Persons and Property Onboard the Aircraft

This section parallels the requirements of those for aircraft operations in the United States. The words ''are carried aboard the aircraft'' are added in this final rule in place of ''board the aircraft,'' which was used in the NPRM, to provide clarification of the scope of covered persons. This technical correction is consistent with the language of FAA regulations at 14 CFR 121.583. The rationale for this addition is described in the Section-by-Section Analysis for § 1544.202.

Section 1546.205 Acceptance and Screening of Cargo

This section clarifies aviation security regulations with respect to the duty of foreign air carriers for the security of air cargo loaded in, or destined for, the United States. TSA amends paragraph (a) and (b), and adds new paragraphs (c), (d), (e), and (f) to § 1546.205. These paragraphs are parallel to those for U.S. aircraft operators in § 1544.205.

Paragraph (d), ''Screening and inspection of cargo in the United States,'' provides that each foreign air carrier must ensure that, as required in its security program, cargo is screened and inspected for any unauthorized persons, and any unauthorized explosives, incendiaries, and other destructive substances or items as provided in the foreign air carrier's security program, in accordance with §§ 1546.207 and 1546.215, if applicable, before loading it on its aircraft in the United States.

Paragraph (e), ''Acceptance of cargo in the United States,'' provides that each foreign air carrier may accept cargo in the United States only from the shipper, or from an aircraft operator, foreign air carrier, or IAC operating under a security program under this chapter, with a comparable cargo security program as provided in its security program.

Paragraph (f) provides that, for cargo to be loaded on its aircraft outside the United States, each foreign air carrier must carry out the requirements of its security program.

Section 1546.213 Security Threat Assessment for Cargo Personnel in the United States

In response to comments, TSA has revised this section from the NPRM to provide greater clarity to the scope of personnel who are required to meet the STA requirements. The rationale for the changes in this section are the same as

stated in the Section-by-Section Analysis for § 1544.228.

Section 1546.215 Known Shipper Program

TSA is codifying the Known Shipper program for foreign air carriers, parallel to the known shipper program applicable to domestic air carriers in § 1544.239. The rationale for adding this section is the same as stated in the Section-by-Section Analysis for § 1544.239.

Section 1546.301 Bomb or Air Piracy Threats

TSA has revised the opening paragraph of this section by deleting the text ''in passenger operations'' and the off-setting commas around this text. This amend provides that foreign air carriers in passenger and all-cargo operations are required to meet parallel security measures as aircraft operators in the same operations.

PART 1548—INDIRECT AIR CARRIER SECURITY

Section 1548.3 TSA Inspection Authority

TSA added § 1548.3(c) to clarify that TSA may enter and be present where an IAC carries out security measures in order to inspect or test compliance, or perform other such duties as TSA may direct.

Section 1548.5 Adoption and Implementation of the Security Program

TSA has revised paragraphs (a), (b), and (c) of § 1548.5 regarding the adoption and implementation of the IACSSP.

Paragraph (a) specifies that no IAC may offer cargo to an aircraft operator operating under a full program or a full all-cargo program specified in part 1544, or to a foreign air carrier conducting a passenger operation under § 1546.101(a) and (b), or an all-cargo program under § 1546.101(e), unless that IAC has and carries out an approved security program under part 1548. Where this part referred to ''employees, agents, contractors, and subcontractors'' in the NPRM, it now reads ''employees and agents.'' This change is not substantive, as contractors and subcontractors are agents with regard to security responsibilities. This change should provide a simplified understanding of persons with security responsibilities.

Paragraph (b) broadens the scope of security measures that may be required in an individual IAC's security program. Consistent with amendments made throughout this final rule, TSA is codifying existing requirements to prevent and deter unauthorized persons from using cargo to access passenger aircrafts. IACs currently having cargo screening responsibilities under current § 1548.5(b)(1) and their approved security programs must ''[p]rovide for the safety of persons and property traveling in air transportation against acts of criminal violence and air piracy and the introduction of any unauthorized explosive or incendiary into cargo aboard a passenger aircraft.'' The IAC now must ''provide for the security of persons and property traveling in air transportation against acts of criminal violence and air piracy and against the introduction of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item as provided in the indirect air carrier's security program.''

This section also broadens the scope of IACs' duties to include cargo to be carried on an aircraft operated under a full all-cargo security program, rather than solely in passenger operations. This change parallels the cargo security requirements in §§ 1544.205 and 1546.205.

Under paragraph (b)(1)(i), this requirement applies from the time the IAC accepts the cargo, to the time it transfers the cargo to an entity that is not an employee or agent of the IAC. This provision clarifies the existing IACSSP requirement that the IAC is responsible for carrying out security measures under this part when its employee or agent fulfills its function. Paragraph (b)(1)(ii) makes clear that security program requirements apply while the cargo is stored, en route, or otherwise being handled by an employee or agent of the IAC. Paragraph (b)(1)(iii) makes clear that security program requirements apply regardless of whether or not the IAC ever has physical possession of the cargo. For example, TSA notes that some IACs conduct their services only through telephone conversations or communications over the computer and use agents to transport the cargo physically. In these circumstances, the person with physical possession on behalf of the IAC is the IAC's agent. When the agent has possession, the IAC remains responsible for ensuring that its security program requirements are met.

Paragraph (b) also requires the IAC to ensure that its employees and agents carry out the requirements of the IACSSP. Thus, TSA's change to paragraph (c) ensures that the content of each IACSSP reflects the scope of security measures established under § 1548.5(b), references known shipper program requirements that are codified in § 1548.17, and establishes a new requirement that each IACSSP include documentation of the procedures and curriculum used to accomplish the training, under § 1548.11, of persons who accept, store, transport or deliver cargo on behalf of the IAC.

Section 1548.7 Approval, Amendment, Annual Renewal, and Withdrawal of Approval of the Security Program

Paragraph (a) reflects that TSA has developed the IACSSP, rather than having each IAC develop its own security program. Thus, consistent with current practices, rather than submitting a security program for TSA approval, an applicant requests approval to operate under the IACSSP. This paragraph explains how an applicant must seek approval to operate under the IACSSP, including a record-keeping requirement, and a list of information that the applicant must submit to TSA for consideration. Paragraph (a) also outlines the process for approving an applicant's operation under a security program, that approvals are effective for one year, and that the approved IAC must notify TSA of changes to the initial application. TSA uses the information submitted by IAC applicants to verify their legitimacy through a check of publicly-available records, and cross checks that information against data on terrorist databases.

Paragraph (b) presents the processes an IAC must follow annually to seek renewed TSA approval to operate under the IACSSP. Annual renewal is a continuation, and codification, of the current practice under the IACSSP. IACs must submit the renewal request to TSA at least 30 calendar days prior to expiration of the IACSSP, as well as other standards for the submission.

Paragraphs (c), (d), and (e) primarily parallel changes made previously to similar requirements for airport operator security programs and aircraft operator security programs in §§ 1542.105 and 1544.105. This section adds a new paragraph (c)(6), allowing a group of IACs to submit a proposed amendment together. Paragraph (d) is the same as the current paragraph (c). Paragraph (d) is separated into three subparagraphs for easier reading. Paragraph (d)(1) substitutes ''aviation security'' for ''safety in air transportation or in air commerce'' to clarify the breadth of TSA's EA authority. Paragraph (d)(2) reorganizes existing EA standards to emphasize immediate effectiveness and that TSA will provide a brief statement regarding the rationale for the EA. Finally, paragraph (d)(3) provides the IAC with 15 days to file a petition for reconsideration but provides that the

filing of the petition does not stay the effective date of the amendment. Paragraph (e) revises the existing Emergency Amendments (EA) standards of the existing paragraph (d).

TSA codifies procedures for TSA to withdraw an IAC's approval to operate under the IACSSP with the addition of paragraph (f). The standard for withdrawal is a TSA determination that the operation is contrary to security and the public interest. Paragraph (f) provides procedures for notice, response, and petition for reconsideration. The affected IAC would be able to request a stay of the withdrawal. TSA also codifies emergency withdrawal procedures. This codification creates procedural guidelines to implement withdrawal of a security program and affords due process to the IAC. The emergency procedures allow the IAC to submit a petition for reconsideration, but the filing of a petition will not stay the effective date of withdrawal.

Paragraph (g) adds provisions for the proper service of documents in the withdrawal proceedings. Procedures for time extensions are found at paragraph (h).

Section 1548.9 Acceptance of Cargo

Paragraph 1548.9(a) broadens the scope of the IAC's duty to prevent or deter the carriage of any unauthorized persons and any unauthorized destructive substances or items on board an aircraft to the existing requirements that focus on preventing and deterring explosives and incendiaries. This provision requires IACs to carry out these procedures whenever offering cargo for air transportation on all-cargo aircraft under a full all-cargo program, as well as on passenger aircraft under a full program. This paragraph adds a requirement that the IAC request the shipper's consent to search or inspect the cargo.

Under the former paragraph 1548.9(b), this duty extended only to cargo that was intended for shipment aboard a passenger aircraft. By removing the word ''passenger,'' this paragraph extends to cargo for shipment aboard certain all-cargo aircraft operations regulated by TSA. Paragraph 1548.9(b) deletes the requirement that the IAC must search or inspect cargo. Such inspections are to be done by the aircraft operator or foreign air carrier only.

Section 1548.11 Training and Knowledge for Individuals with Security-Related Duties

Certain employees and agents of IACs are subject to security-related training. These enhanced requirements for training cover individuals who perform security-related duties to ensure the appropriate security standards are met.

Paragraph 1548.11(a) specifies that an IAC must not use any individual to perform any security-related duties to meet the requirements of its security program unless the individual has received training as specified in its security program. This requirement covers employees and agents performing security-related duties for the IAC.

Under § 1548.11(b), additional training requirements are specified for individuals who accept, handle, transport, or deliver cargo for or on behalf of the IAC. This training must include, at a minimum, requirements contained in the applicable provisions of part 1548, applicable Security Directives and Information Circulars, the approved airport security program applicable to their location, and the aircraft operator's or IAC's security program to the extent that such individuals need to know in order to perform their duties.

Paragraph 1548.11(c) requires annual recurrent training of covered individuals in these elements of knowledge. Pursuant to § 1548.7(a), initial training of the identified individuals performing duties for the IAC must be completed before an IAC may begin operations under its approved security program. TSA is providing a training curriculum to the IAC in this regard.

Section 1548.13 Security Coordinators

TSA requires each IAC to designate and use an Indirect Air Carrier Security Coordinator (IACSC). The IAC is required to appoint the IACSC at the corporate level, and the IACSC is the IAC's primary contact for security-related activities and communications with TSA, as set forth in the IACSSP. Either the IACSC or an alternate IACSC must be available on a 24-hour basis. This addition parallels existing security coordinator positions required of airport operators in § 1542.3 and aircraft operators in § 1544.215.

Section 1548.15 Security Threat Assessments for Individuals Having Unescorted Access to Cargo

TSA has provided revisions to this section consistent with the scope of the NPRM. This section is significantly restructured in order to be responsive to comments and provide greater clarity to the scope of personnel who are required to meet the STA requirements. The rationale for the changes in this section are the same as stated in the Section-by-Section Analysis for § 1544.228.

Section 1548.16 Security Threat Assessments for Each Proprietor, General Partner, Officer, Director, and Specified Owner of the Entity

TSA has added this section to provide reference within part 1548 to the STA requirement at § 1540.209(a). TSA has provided further clarification to the scope of persons covered under this section such as to cover partnerships and proprietors. In large part, TSA has adopted the meaning of ''owner,'' ''same family,'' and ''voting securities and other voting interests'' as are found at 31 CFR 103.175, for regulation of foreign banks.

Section 1548.17 Known Shipper Program

Section 1548.17 codifies the Known Shipper program in regulation. This addition is essentially the same as that for aircraft operators under proposed § 1544.239.

Section 1548.19 Security Directives and Information Circulars

This section provides a procedure for TSA to issue emergency security measures to IACs through Security Directives (SD). This section authorizes TSA to issue Security Directives and Information Circulars to regulated IACs, and mandates compliance by the IAC with each Security Directive that it receives. Section 1548.19 also requires the IAC to acknowledge in writing receipt of the SD within the time prescribed in the SD, and to specify the method by which the measures in the SD have been implemented (or will be implemented, if the SD is not yet effective) within the time prescribed in the SD. In the event that the IAC is unable to implement the measures in a SD, § 1548.19 authorizes the IAC to submit proposed alternative measures and the basis for the alternative measures to TSA for approval. The IAC must submit the proposed alternative measures within the time prescribed in the SD and, if they are approved by TSA, the IAC must implement them.

Section 1548.19 also provides that each IAC that receives a SD may comment on the SD by submitting data, views, or arguments in writing to TSA, and that TSA may amend the SD based on comments received. Section 1548.19 also provides that submission of a comment does not delay the effective date of the SD.

Section 1548.19 also provides that each IAC that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular must restrict the availability of

the Security Directive or Information Circular, and information contained in either document, to those persons with a need-to-know. The IAC must 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.

IV. Fee Authority for Security Threat Assessment

On October 1, 2003, legislation was enacted requiring TSA to collect reasonable fees to cover the costs of providing credentialing and background investigations in the transportation field.[22] Fees collected under this legislation (Section 520) may be used to pay for the costs of conducting or obtaining a criminal history records check (CHRC); reviewing available law enforcement databases, commercial databases, and records of other governmental and international agencies; reviewing and adjudicating requests for waivers and appeals of TSA decisions; and any other costs related to performing a background records check or providing a credential.

Section 520 mandates that any fee collected shall be available for expenditure only to pay for the costs incurred in providing services in connection with performing a background check or providing a credential. The fee shall remain available until expended. TSA is establishing this fee in accordance with the criteria set forth in 31 U.S.C. 9701 (General User Fee Statute), which requires fees to be fair and based on (1) costs to the government, (2) the value of the service or thing to the recipient, (3) public policy or interest served, and (4) other relevant facts.

Summary of Security Threat Assessment Requirement

TSA currently requires a variety of individuals working in aviation to submit to criminal history records checks to reduce the likelihood that a terrorist would gain employment that would give them access to the aircraft. Generally, these individuals work on airport grounds and have unescorted access to secure areas. In the cargo environment, many other persons have access to cargo before someone who has had such a check handles it. TSA recognizes that the number of individuals with unescorted access to cargo is very large and that extending fingerprint-based records checks to all of these people would likely be a very time-consuming and costly process that would cause a major disruption to the domestic and international transportation of goods. TSA focused the STA program on a review of terrorist databases to determine whether individuals seeking unescorted access to cargo present a terrorist threat.

Flexibility will be achieved by ensuring that each of the following individuals are required to have either an STA or a background check for unescorted SIDA access authority. The covered individuals include:

(1) Each proprietor, general partner, officer, director, and owner identified under § 1548.16 of an IAC, or applicant to be an IAC.

(2) Each employee and agent authorized to have unescorted access to cargo where:

- Aircraft operators with a full program and foreign air carriers under § 1546.101(a) or (b) accept cargo;
- Aircraft operators with a full all-cargo program and foreign air carriers under § 1546.101(e) consolidate or inspect cargo;
- IACs accept cargo for transportation on aircraft operated by an aircraft operator with a full program or a foreign air carrier under § 1546.101(a) or (b); or
- IACs consolidate or hold cargo for transportation aboard an aircraft operated by an aircraft operator with a full or full all-cargo program, or a foreign air carrier under § 1546.101(a), (b), or (e).

Security Threat Assessment Population

The above-referenced personnel who are authorized to have unescorted access to cargo on behalf of an IAC, an aircraft operator, or a foreign air carrier would be required to undergo a name-based STA. TSA approximates a ''de minimis'' number of persons who own 25 percent or more of these IACs that are not also officers or directors of the entity. Accordingly, TSA has not accounted for these individuals separately. However, those personnel with unescorted SIDA access already have undergone a criminal history records check. TSA would accept the criminal history records check in lieu of the proposed STA for these personnel.

The Indirect Air Carrier Population

TSA estimates that there are approximately 5,000 companies that are defined as IACs under this rule. TSA further estimates that there are, on average, approximately 13 employees per IAC, of whom an average of 10 would typically require regular unescorted access to air cargo and thus would need an STA under this rule. Therefore, the total IAC population requiring an STA is estimated to be 50,000 (5,000 x 10). Further discussion of TSA's IAC population estimates can be found in the full Regulatory Evaluation.

Cargo Personnel Not Subject to Other TSA Security Threat Assessments

TSA estimates that there are approximately 65 aircraft operators and foreign air carriers operating all-cargo flights that have employees who are subject to the proposed STA. As discussed in the Regulatory Evaluation aircraft operators and foreign air carriers have some employees who are required to submit to the fingerprint-based SIDA check, while others will only be required to submit to an STA. Because most of the aircraft operator employees are already covered by the SIDA background check requirements, TSA believes that only a limited number of employees would be required to submit to an STA. TSA estimates that there are, on average, approximately 25 employees for each aircraft operator and foreign air carrier operating all-cargo flights who would be required to submit to an STA. Therefore this total population is estimated to be 1,625 (65 x 25). Further discussion of TSA's estimates for affected all-cargo employees can be found in the full Regulatory Evaluation.

Total Initial Population

Given the estimated IAC population of 50,000 and 1,625 additional employees of relevant aircraft operators and foreign air carriers operating all-cargo flights, the total population subject to an STA is 51,625. This is the initial population TSA estimates will be required to submit to an STA during the first year of the program.

Recurring Population

TSA estimates approximately 15 percent of the initial total population will be required to submit to an STA each year after the initial assessment. Further discussion of TSA's recurring population estimate can be found in the full Regulatory Evaluation. This percentage represents annual new employers or employees with a new requirement for the STA. Therefore, the recurring population that would be required to submit to an STA annually is estimated to be 7,744 (15 percent x 51,625).

Five Year Population

Given the first year estimated population of 51,625 and subsequent annual recurring population of 7,744, TSA estimates the total population

[22] Department of Homeland Security Appropriations Act, 2004, Sec. 520 (Pub. L. 108–90, Oct. 1, 2003, 117 Stat. 1137).

receiving an STA over the first 5 years to be 82,601 (51,625 + (4 x 7,744)). TSA employs a five-year population period for calculating the STA fee to distribute the costs of delivering these services to the entire population more equitably, as required under this rule.

Program Costs

This section summarizes TSA's estimated costs for establishing the program, processes, and resources necessary to establish and perform the STA on the population as required under this rule.

Leveraging Existing Resources

Where possible, TSA will leverage processes, infrastructure and personnel that are currently utilized for other federal government air cargo regulatory initiatives and threat assessment services. These efforts will minimize the need for new government expenditures and keep fee levels to a minimum. For example, TSA is expanding its existing IAC database management system, currently used to manage regulatory relationships with IACs that ship cargo on passenger aircraft, to be able to collect and process the required applicant information from air cargo employees and agents that require an STA. Moreover, TSA is leveraging other existing applicant vetting processes and infrastructure, which TSA threat assessment programs benefit from collectively, so as not to create overlapping resource requirements.

Start-Up Costs

The startup costs are not incorporated in fee calculations. TSA has made this determination because these expenses are largely the result of extending information systems already built for other regulatory activities within the air cargo/IAC industry. As such, TSA is not including these startup costs in the fee.

Five-Year Recurring Costs

The entire population covered under this rule must submit to an STA within 180 days of rule publication, and thereafter only a small fraction (15 percent) of applications are expected annually. TSA must ensure that the fixed costs of the program are not borne solely by the smaller pool of new applicants in Year 1. Therefore, TSA averages the estimated total five-year recurring program costs and divides this value by the estimated five-year STA population to generate its per applicant fee.

TSA estimates the five-year recurring costs to be $2,322,702. These costs include $1,837,500 for all required program personnel, $320,000 for all information management and hardware/software costs, and $165,202 for all vetting process costs. See Figure 1 below for additional details.

FIGURE 1.—TSA SECURITY THREAT ASSESSMENT PROGRAM COSTS ESTIMATES

Category and sub-category	Description	Year 1	Years 2–5	Five-year recurring costs
Hardware/Software:				
IAC MS Database System Modifications	Modification of existing IAC/air cargo database to accommodate new Security Threat Assessment (STA) information management requirements. Annual recurring system expense estimated to be 10 percent of start-up modification costs.	$0	$70,000	$280,000
Screening Gateway Interface Development	Modification of existing interface to conform to program needs. Annual recurring system expense estimated to be 10 percent of start-up modification costs.	0	10,000	40,000
System Security Testing, Set-up and Hosting.	Costs related to system set-up required for application hosting.	0	0	0
Hardware/Software Total		0	80,000	320,000
Support Functions:				
Additional Program Personnel	Two additional federal employee full-time equivalents (FTEs) will be required to perform functions associated with the STA. Total cost to TSA is estimated at $105,000 per FTE (fully loaded, including administrative overhead costs).	210,000	210,000	1,050,000
Finance/Accounting Personnel	One half of an FTE (.5) will be required to perform accounting and reconciliation functions and provide financial reports to program personnel. Total cost to TSA is estimated at $105,000 per FTE (fully loaded, including administrative overhead costs).	52,500	52,500	262,500
Support Functions Total		262,500	262,500	1,312,500
Security Threat Assessment:				
Threat Assessment Analysis	A security threat analysis is the process of querying applicant names against various terrorism-related government sources. This cost is derived by multiplying the total estimated program population by the TSA's estimated cost of $2 per applicant. Assumes 15 percent annual employee turnover.	103,250	15,488	165,202

FIGURE 1.—TSA SECURITY THREAT ASSESSMENT PROGRAM COSTS ESTIMATES—Continued

Category and sub-category	Description	Year 1	Years 2–5	Five-year recurring costs
Threat Assessment Process Personnel	One additional FTE at $105,000 annually will be necessary to provide support for background check component. Will also perform support functions. Total cost to TSA is estimated at$105,000 per FTE.	105,000	105,000	525,000
Security Threat Assessment Total	.....	208,250	120,488	690,202
Total Costs	.....	470,750	462,988	2,322,702

Cost Adjustments

Pursuant to the Chief Financial Officers Act of 1990, DHS/TSA will review this fee at least every two years.[23] Upon review, if it is found that the fee is either too high (*i.e.*, total fees exceed the total cost to provide the services) or too low (*i.e.*, total fees do not cover the total costs to provide the services), TSA may propose changes to the fees. In addition, as DHS and TSA identify and implement additional efficiencies across numerous threat assessment and credentialing programs, resulting cost savings will be incorporated into the fee levels accordingly.

Fee Calculation

TSA is charging a fee to cover the recurring costs of the program. TSA estimates that total recurring program costs for the first 5 years (not including start-up costs) will be approximately $2,322,702 (($470,750 + (462,988 × 4)). These total costs, divided by the estimated five-year total of 82,601 applicants, yields a per applicant fee of $28 ($2,322,702/82,601), rounded down from $28.12.

Fee Remittance Process

TSA will employ a third party to establish the infrastructure for collecting the required financial data and fees for forwarding to TSA. This process will function in a similar manner to that of other TSA threat assessment programs and may include the services of Pay.gov, *https://www.pay.gov/paygov/,* the government-wide solution for Internet-based online payment services.

V. Rulemaking Analyses and Notices

V.A. Regulatory Evaluation Summary

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866 directs each Federal agency to propose or adopt a regulation only if the agency makes a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 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. In developing U.S. standards, this Trade Act requires agencies to consider international standards and where appropriate, as the basis of U.S. standards. Fourth, the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4) 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).

In conducting these analyses, TSA has determined this rule—

(1) Is a ''significant regulatory action'' as defined in Executive Order 12866;

(2) Will not have a significant impact on a substantial number of small entities;

(3) Imposes no significant barriers to international trade; and

(4) Does not impose an unfunded mandate on State, local, or tribal governments, but does on the private sector.

Because TSA has determined that this rule is a significant regulatory action under Executive Order 12866, this rule has been reviewed and approved by the Office of Management and Budget (OMB).

Economic Impacts

This summary highlights the costs and benefits of the final rule to amend the transportation security regulations to further enhance and improve the security of air cargo transportation. TSA has determined that this is a major rule within the definition of Executive Order 12866, as annual costs or benefits to all parties do pass the $100 million threshold in any year. There are no significant economic impacts for each of the required analyses of small business impact, international trade, or unfunded mandates.

Details of the proposed rule and the associated analysis were provided to the public for comment. This final regulatory analysis covers changes to the previous analysis in response both to public comments and changes TSA has made with the final rule. The complete analysis and the associated references are not repeated here. The required OMB Circular A–4 accounting statement is presented in the full regulatory evaluation, which is available in the docket as ''Final Regulatory Evaluation, Regulatory Flexibility Determination, Trade Impact Assessment, and Unfunded Mandate Assessment.''

Costs

The following sections summarize the estimated costs of this rulemaking by general category of who pays. A detailed summary table in the full regulatory evaluation provides an overview of the cost items, section of the regulation that creates the requirement, and a description of cost elements. Both in this summary and the economic evaluation, descriptive language is used to try and relate the consequences of the regulation. Although the regulatory evaluation attempts to mirror the terms and wording of the regulation, no attempt is made to precisely replicate the regulatory language and readers are cautioned that the actual regulatory text, not the text of the evaluation, is binding. Throughout the evaluation rounding in displayed values may result in minor differences in displayed totals.

Aircraft Operators will incur additional costs to comply with requirements of this rulemaking over

[23] 31 U.S.C. 902.

the 10-year period of 2005–2014. Cargo aircraft operators are estimated to incur costs totaling approximately $1.9 billion to comply with the requirements to require background checks for individuals who screen cargo for all-cargo aircraft, their supervisors, as well as for employees with unescorted access to the cargo. The rulemaking requires all-cargo aircraft operators to screen all persons entering the aircraft. This requirement is estimated to impose costs of approximately $35.2 million over the ten-year period of this analysis. They also are required to take additional measures to secure the aircraft and facilities at an estimated cost of $0.8 million. All-cargo aircraft operators with a maximum certificated take-off weight greater than 45,500 kg (100,309.3 lbs) need to ensure they have coordinated law enforcement notification and response capability to comply with the requirements to extend or create new secure areas to encompass air cargo operations. This requirement is not an expansion of law enforcement staffing. As a result, costs previously attributed to the LEO function have been removed. Finally, the codifying of existing Security Directive requirements and costs for random screening of air cargo on passenger aircraft and all-cargo flights are estimated to cost of $1.491 billion, and $328 million, respectively. Much of this increase is related to increased screening levels as mandated by Congress.

Airport Operators that have one or more SIDAs are required to extend or create a new SIDA to encompass air cargo operations. This change applies only to aircraft operations conducted with aircraft having a maximum certificated take-off weight greater than 45,500 kg (100,309.3 lbs) operating a full program or a full all-cargo security program. TSA estimates the cost of this requirement to be $10.9 million over the ten-year period of this analysis. This cost reflects the cost of additional employee badges, additional airports, and the administrative costs of updating the airports' security plans.

Indirect Air Carriers are impacted in several ways by this rulemaking. They are now required to complete security threat assessments for certain individuals. This requirement is estimated to impose costs totaling $4.6 million over ten years. IACs are also required to implement training and develop a testing tool for individuals who perform security related duties to meet the requirements of their security programs. These costs are estimated at $35.2 million over the ten-year period 2005–2014. They include the cost of initial training for the entire IAC labor force and annual recurrent training for the IAC labor force. This rulemaking establishes new requirements for IACs to obtain approval, to amend, and for annual recertification of their security programs. The costs estimated to comply with these requirements are $43.9 million over the period of this analysis.

Foreign Air Carriers costs inside the United States are considered domestic costs for the purpose of this analysis and, therefore, are not estimated separately from domestic carrier costs; a separate discussion for these costs is not included. This costing method reflects the way the Department of Transportation reports data on foreign aircraft operations in the U.S. and the way it reports the cost impact of such aircraft operations on the U.S. economy. Security requirements of this rulemaking apply equally to foreign air carriers just as they apply to domestic carriers. For their overseas operations, individual foreign carriers are expected to experience financial impacts at levels similar to those experienced by domestic carriers and are not estimated here.

TSA will incur costs as a result of the rule. Development of training for IAC employees will cost the agency approximately $450K. TSA also will incur costs of approximately $24.5 million to administer the Known Shipper program. The cost to TSA for the vetting of IACs is estimated at $2.6 million. TSA will also be modifying its current IAC compliance management system to accommodate the Security Threat Assessments in this rule. The costs of utilizing this system and some STA support costs are captured in the unit costs used to develop the fee costs for the aircraft operators and indirect air carriers.

In summary, the cost impacts of this rulemaking are estimated to total approximately $2.0 billion undiscounted (discounted: $1.5 billion at 7 percent, $1.8 billion at 3 percent), over the period 2005–2014. Aircraft operators will incur costs totaling $1.9 billion, airport operators $10.9 million, IACs $83.6 million and TSA anticipates cost expenditures to administer the provisions of the rulemaking at $27.6 million over the ten year analysis period. Details on how estimates were developed, as well as the discounted value comparisons, were presented in the original evaluation. A separate Final Regulatory Evaluation is available on the docket and details the changes from the Initial Regulatory Evaluation. The full evaluation also includes detailed tables showing constant dollars; discounted costs at 7 percent and 3 percent; and a table of changes from the NPRM.

Final Regulatory Flexibility Analysis (FRFA)

The Regulatory Flexibility Act of 1980 (RFA) establishes ''as a principle of regulatory issuance that agencies shall endeavor, consistent with the objective of the rule and of applicable statutes, to fit regulatory and informational requirements to the scale of the business, organizations, and governmental jurisdictions subject to regulation.'' To achieve that principle, the RFA requires agencies to solicit and consider flexible regulatory proposals and to explain the rationale for their actions. The RFA covers a wide range of small entities, including small businesses, not-for-profit organizations, and small governmental jurisdictions.

Agencies must perform a review to determine whether a proposed or final rule will have a significant economic impact on a substantial number of small entities. If the determination is that it will, the agency must prepare a regulatory flexibility analysis as described in the Act.

However, if an agency determines that a proposed or final rule is not expected to have a significant economic impact on a substantial number of small entities, section 605(b) of the 1980 RFA provides that the head of the agency may so certify and a regulatory flexibility analysis is not required. The certification must include a statement providing the factual basis for this determination, and the reasoning should be clear.

TSA conducted the required initial review of this rule and indicated that TSA believed it would not have a significant economic impact on a substantial number of small entities. There are two primary sources of change related to the RFA analysis. Although IAC costs in total went up, the population of both workers and businesses both went up. The cost impact per employee and business unit were calculated and summed to get a total business cost per business. TSA examined the smallest businesses' revenue and compared the cost as a percent of the revenue. This calculation in the Initial Regulatory Flexibility Analysis rounded to 0.0 percent. When recomputed in the Final Regulatory Flexibility Analysis (FRFA) the same computation still rounds to 0.0 percent. Therefore, TSA finds that there is not a significant impact on a substantial number of small businesses. More detail on the FRFA can be found in the separate Final Regulatory Evaluation, available on the docket.

V.B. Paperwork Reduction Act

TSA did not receive comments that provided substantive information for consideration regarding the Paperwork Reduction Act. Under the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501, *et seq.*), a Federal agency must obtain approval from OMB for each collection of information it conducts, sponsors, or requires through regulations. This proposal contains information collection activities subject to the PRA. Accordingly, the following information requirements are being submitted to OMB for its review.

Title: Air Cargo Security Requirements.

Summary: TSA is amending the transportation security regulations to further enhance and improve the security of air cargo transportation. Specifically, TSA is creating a mandatory security program for all-cargo aircraft operations over 45,500 kg (100,309.3 lbs.) and is amending existing security regulations and programs for aircraft operators, foreign air carriers, airport operators, and IACs. TSA is expanding STA requirements to new populations, including certain individuals who have unescorted access to air cargo, each proprietor, general partner, officer, and director, and certain owners of an IAC or applicant to be an IAC.

Use of: Security programs that are developed or amended as a result of this final rule will be kept on file and updated so that TSA inspectors may check for regulatory compliance and uniform application of the rules. Evidence of appropriate employee training in security matters will also become a part of this record. STAs conducted as a result of this final rule will be used to determine employment suitability for those who have unescorted access to cargo and each proprietor, general partner, officer, and director, and certain owners of an IAC or applicant to be an IAC. Similarly, employees and agents of aircraft operators must successfully complete a CHRC prior to screening cargo.

Respondents (including number of): The respondents to this information requirement are aircraft operators, foreign air carriers, IACs, and their employees who undergo STAs for a total of approximately 51,625 respondents the first year and approximately 7,744 respondents each following year, for an average of 22,371 respondents for each of the three years. Respondents also include carriers and their employees who undergo CHRCs, for a total of approximately 50,000 respondents the first year and approximately 7,651 each following year, for an average of 21,742 respondents for each of the three years. The combined average number of respondents for STAs and CHRCs is approximately 49,395 for each of the three years. The annual number of respondents includes both new entrants and renewals. The number consists of 65 all-cargo operators, 5,000 IACs, and their affected employees. TSA made these estimates after reviewing public comments.

Frequency: Upon implementation, security programs related to this final rule, including employee training records, will need to be kept on file and updated as necessary. STAs will be conducted for all existing and subsequent new employees who have unescorted access to cargo where such employees do not already have unescorted SIDA access. CHRCs will be conducted on individuals who are employees of aircraft operators and who have the responsibility to screen cargo.

Annual Burden Estimate: The annual burden associated with the security program is estimated to be 43,143 hours. The annual burden associated with the STA is estimated to average 5,593 hours over the three years, while the annual burden associated with the CHRCs is estimated to average 10,871 hours over the three years for a combined average annual total of 59,607 hours.

The agency invited 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 through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

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. The OMB control number for this information collection will be published in the **Federal Register** after OMB approves it.

V.C. International Compatibility

In keeping with United States obligations under the Convention on International Civil Aviation, it is TSA policy to comply with International Civil Aviation Organization (ICAO) Standards and Recommended Practices to the maximum extent practicable. TSA has determined that these regulations are consistent with ICAO Standards and Recommended Practices.

V.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 final rule and has determined that carrier operations at overseas locations must provide an equivalent level of security. At most the impact of this rule creates an even competitive cost structure.

V.E. Unfunded Mandates Reform Act Analysis

The Unfunded Mandates Reform Act of 1995 (the Act) is intended, among other things, to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of the Act 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 final rule does not contain such a mandate on State, local, and tribal governments. The overall impact on the economy does exceed the threshold in the aggregate. The full regulatory evaluation documents costs, public comments, alternatives, and TSA accommodation of the public comments.

V.F. 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 would not have a substantial direct effect on the States, on 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 would not have federalism implications.

V.G. Environmental Analysis

TSA has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4347) and has determined that this action will not have a significant effect on the human environment. In accordance with FAA Order 1050.1D, appendix 4, paragraph 4(j), this rulemaking action qualifies for a categorical exclusion. The FAA order continues to apply to TSA in accordance with the Homeland Security Act (Pub. L. 107–296), until DHS publishes its NEPA implementing regulations.

V.H. Energy Impact

The energy impact of this document has been assessed 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.

VI. List of Subjects

49 CFR Part 1520

Air transportation, Law enforcement officers, 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.

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 1548

Air transportation, Reporting and recordkeeping requirements, Security measures.

VII. The Amendment

■ For the reasons set forth above, the Transportation Security Administration amends title 49 of the Code of Federal Regulations parts 1520, 1540, 1542, 1544, 1546, and 1548 to read as follows:

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

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

Authority: 49 U.S.C. 114, 5103, 40119, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

■ 2. Amend § 1520.5 by revising paragraphs (b)(2)(i), (b)(3)(i), and (b)(4)(i) to read as follows:

§ 1520.5 Sensitive security information.

* * * * *

(b) * * *

(2) * * *

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority;

* * * * *

(3) * * *

(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority; and

* * * * *

(4) * * *

(i) Any device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

* * * * *

SUBCHAPTER C—CIVIL AVIATION SECURITY

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

■ 3. 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.

■ 4. Amend § 1540.5 by revising the definition of ''indirect air carrier'' and adding a new definition of ''unescorted access to cargo'' in alphabetical order to read as follows:

§ 1540.5 Terms used in this subchapter.

* * * * *

Indirect air carrier (IAC) means any person or entity within the United States not in possession of an FAA air carrier operating certificate, that undertakes to engage indirectly in air transportation of property, and uses for all or any part of such transportation the services of an air carrier. This does not include the United States Postal Service (USPS) or its representative while acting on the behalf of the USPS.

* * * * *

Unescorted access to cargo means the authority granted by an aircraft operator or IAC to individuals to have access to air cargo without an escort.

■ 5. Amend § 1540.111 by revising paragraph (a)(1) to read as follows:

§ 1540.111 Carriage of weapons, explosives, and incendiaries by individuals.

(a) * * *

(1) When performance has begun of the inspection of the individual's person or accessible property before entering a sterile area, or before boarding an aircraft for which screening is conducted under this subchapter;

* * * * *

■ 6. Add new Subpart C—Security Threat Assessments to read as follows:

Subpart C—Security Threat Assessments

Sec.

Subpart C—Security Threat Assessments

§ 1540.201 Applicability and terms used in this subpart.

(a) This subpart includes the procedures that certain aircraft operators, foreign air carriers, and indirect air carriers must use to have security threat assessments done on certain individuals pursuant to 49 CFR 1544.228, 1546.213, 1548.7, 1548.15, and 1548.16. This subpart applies to—

(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 1548; and

(4) Each individual with, or applying for, unescorted access to cargo under one of the programs described in (a)(1) through (a)(3) of this section.

(5) Each proprietor, general partner, officer, director, or owner of an indirect air carrier as described in 49 CFR 1548.16.

(b) For purposes of this subpart—

Individuals means the individuals listed in paragraphs (a)(4) and (a)(5) of this section.

Operator means an aircraft operator, foreign air carrier, and indirect air carrier listed in paragraphs (a)(1) through (a)(3) of this section.

(c) An individual poses a security threat under this subpart when TSA determines that he or she is known to pose or suspected of posing a threat—

(1) To national security;
(2) To transportation security; or
(3) Of terrorism.
(d) For purposes of this subpart:
(1) *Date of service* means—
(i) The date of personal delivery in the case of personal service;
(ii) The mailing date shown on the certificate of service;
(iii) The date shown on the postmark if there is no certificate of service;
(iv) Another mailing date shown by other evidence if there is no certificate of service or postmark; or
(v) The date in an e-mail showing when it was sent.
(2) *Day* means calendar day.

§ 1540.203 Operator responsibilities.

(a) Each operator subject to this subpart must ensure that each individual described in § 1540.201(a)(4) and (a)(5) completes the Security Threat Assessment described in this section.
(b) Each operator must:
(1) Authenticate the identity of the individual by—
(i) Reviewing two forms of identification, one of which must be a government-issued picture identification; or
(ii) Other means approved by TSA.
(2) Submit to TSA a Security Threat Assessment application for each individual that is signed by the individual and that includes:
(i) Legal name, including first, middle, and last; any applicable suffix; and any other names used previously.
(ii) Current mailing address, including residential address if it differs from the current mailing address, and all other residential addresses for the previous five years, and e-mail address, if the individual has an e-mail address.
(iii) Date and place of birth.
(iv) Social security number, (submission is voluntary, although recommended).
(v) Gender.
(vi) Country of citizenship, and if naturalized in the United States, date of naturalization and certificate number.
(vii) Alien registration number, if applicable.
(viii) The following statement reading:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 49 U.S.C. 5103a. *Purpose:* This information is needed to verify your identity and to conduct a Security Threat Assessment to evaluate your suitability for completing the functions required by this position. Failure to furnish your SSN may result in delays in processing your application, but will not prevent completion of your Security Threat Assessment. Furnishing the other information is also voluntary; however, failure to provide it may delay or prevent the completion of your Security Threat Assessment, without which you may not be granted authorization to have unescorted access to air cargo subject to TSA security requirements. *Routine Uses:* Routine uses of this information include disclosure to TSA contractors or other agents who are providing services relating to the Security Threat Assessments; to appropriate governmental agencies for law enforcement or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement. For further information, please consult DHS/TSA 002 Transportation Security Threat Assessment System.

The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact, on this application can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of authorization or in the case of parties regulated under this section, removal of authorization to operate under this chapter, if applicable.

(3) Retain the individual's signed Security Threat Assessment application and any communications with TSA regarding the individual's application, for 180 days following the end of the individual's service to the operator.
(c) Records under this section may include electronic documents with electronic signature or other means of personal authentication, where accepted by TSA.

§ 1540.205 Notification.

(a) *TSA review.* In conducting the Security Threat Assessment, TSA reviews—
(1) The information required in § 1540.203(b) and transmitted to TSA; and
(2) Domestic and international databases relevant to determining whether an individual poses a security threat or that confirm an individual's identity.
(b) *Determination of No Security Threat.* TSA serves a Determination of No Security Threat on the individual and the operator, if TSA determines that an individual does not pose a security threat.
(c) *Initial Determination of Threat Assessment.* TSA serves an Initial Determination of Threat Assessment on the individual and the operator, if TSA determines that the individual poses a security threat. The Initial Determination of Threat Assessment includes—
(1) A statement that TSA has determined that the individual poses a security threat;
(2) The basis for the determination;
(3) Information about how the individual may appeal the determination; and
(4) A statement that if the individual chooses not to appeal TSA's determination within 30 days of receipt of the Initial Determination of Threat Assessment in accordance with § 1540.207, or does not request an extension of time within 30 days of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination of Threat Assessment becomes a Final Determination of Threat Assessment.
(d) *Final Determination of Threat Assessment.* If TSA determines that an individual poses a security threat, TSA serves a Final Determination of Threat Assessment on the operator and the individual who appealed the Initial Determination of Threat Assessment.
(e) *Withdrawal by TSA.* TSA serves a Withdrawal of the Initial Determination of Threat Assessment on the individual and a Determination of No Security Threat on the operator, if the appeal results in a determination that the individual does not pose a security threat.

§ 1540.207 Appeal procedures.

(a) *Scope.* This section applies to individuals who wish to appeal an Initial Determination of Threat Assessment.
(b) *Grounds for Appeal.* An individual may appeal an Initial Determination of Threat Assessment if the individual is asserting that he or she does not pose a security threat.
(c) *Appeal.* An individual initiates an appeal by submitting a written reply or written request for materials from TSA or by requesting more time in accordance with § 1540.205(c)(4). If the individual fails to initiate an appeal within 30 days of receipt, the Initial Determination of Threat Assessment becomes final, and TSA serves a Final Determination of Threat Assessment on the operator and the individual.
(1) *Request for materials.* An individual receiving an Initial Determination of Threat Assessment may serve upon TSA a written request for copies of the materials upon which the Initial Determination of Threat Assessment was based.
(2) *TSA response.* Within 30 days of receiving the individual's request for materials, TSA serves copies upon the individual of the releasable materials upon which the Initial Determination of Threat Assessment was based. TSA will exclude any classified information or other protected information described in paragraph (f) of this section.

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

(i) The individual may contact the jurisdiction or entity responsible for the information and attempt to correct or complete information contained in his or her record.

(ii) The individual must then provide TSA with the revised record, or a certified true copy of the information from the appropriate entity, before TSA may determine that the individual meets the standards for the Security Threat Assessment.

(4) *Reply.* (i) The individual may serve upon TSA a written reply to the Initial Determination of Threat Assessment within 30 days of service of the Initial Determination of Threat Assessment, or 30 days after the date of service of TSA's response to the individual's request for materials under paragraph (c)(1) of this section, if the individual served such a request.

(ii) In an individual's reply, TSA will consider only material that is relevant to verifying identification or determining that the individual does not pose a security threat.

(5) *Final determination.* Within 30 days after TSA receives the individual's reply, TSA serves a Final Determination of Threat Assessment or a Withdrawal of the Initial Determination of Threat Assessment.

(d) *Final Determination of Threat Assessment.* (1) If TSA determines that the individual poses a security threat, TSA serves a Final Determination of Threat Assessment upon the individual and the operator. The Final Determination of Threat Assessment includes—

(2) A statement that TSA has reviewed the Initial Determination of Threat Assessment, the individual's reply, if any, and any other materials or information available to him or her and has determined that the individual poses a security threat.

(e) *Withdrawal of Initial Determination of Threat Assessment.* If TSA concludes that the individual does not pose a security threat, TSA serves a Withdrawal of the Initial Determination of Threat Assessment on the individual and the operator.

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

(g) *Extension of time.* TSA may grant an individual an extension of time of the limits set forth in this section for good cause shown. An individual's request for an extension of time must be in writing and be received by TSA at least 2 days before the due date to be extended. TSA may grant itself an extension of time for good cause.

(h) *Judicial review.* The Final Determination of Threat Assessment constitutes a final TSA order subject to judicial review in accordance with 49 U.S.C. 46110.

§ 1540.209 Security threat assessment fee.

(a) *Imposition of fees.* The fee of $28 is required for TSA to conduct a security threat assessment for an individual.

(b) *Remittance of fees.* (1) The fee required under this subpart must be remitted to TSA, in a form and manner acceptable to TSA, each time the individual or an aircraft operator, foreign air carrier, or indirect air carrier submits the information required under § 1540.203 to TSA.

(2) Fees remitted to TSA under this subpart must be payable to the ''Transportation Security Administration''' in U.S. currency and drawn on a U.S. bank.

(3) TSA will not issue any fee refunds, unless a fee was paid in error.

PART 1542—AIRPORT SECURITY

■ 7. The authority citation for part 1542 continues to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44905, 44907, 44913–44914, 44916–44917, 44935–44936, 44942, 46105.

■ 8. Amend § 1542.1 by adding new paragraph (d) to read as follows:

§ 1542.1 Applicability of this part.

* * * * *

(d) Each airport operator that does not have a security program under this part that serves an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter. Such airport operators must comply with § 1542.5(e).

■ 9. Amend § 1542.5 by adding paragraph (e) to read as follows:

§ 1542.5 Inspection authority.

* * * * *

(e) TSA may enter and be present at an airport that does not have a security program under this part, without access media or identification media issued or approved by an airport operator or aircraft operator, to inspect an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter.

■ 10. Amend § 1542.101 by revising paragraphs (a) introductory text, (b), and (c) introductory text to read as follows:

§ 1542.101 General requirements.

(a) No person may operate an airport subject to § 1542.103 unless it adopts and carries out a security program that—

* * * * *

(b) Each airport operator subject to § 1542.103 must maintain one current and complete copy of its security program and provide a copy to TSA upon request.

(c) Each airport operator subject to § 1542.103 must—

* * * * *

■ 11. Amend § 1542.205 by revising paragraphs (a) and (b)(2), and adding new paragraph (c) to read as follows:

§ 1542.205 Security of the security identification display area (SIDA).

(a) Each airport operator required to have a complete program under § 1542.103(a) must establish at least one SIDA, as follows:

(1) Each secured area must be a SIDA.

(2) Each part of the air operations area that is regularly used to load cargo on, or unload cargo from, an aircraft that is operated under a full program or a full all-cargo program as provided in § 1544.101(a) or (h) of this chapter, or a foreign air carrier under a security program as provided in § 1546.101(a), (b), or (e), must be a SIDA.

(3) Each area on an airport where cargo is present after an aircraft operator operating under a full program or a full all-cargo program under § 1544.101(a) or (h) of this chapter, or a foreign air carrier operating under a security program under § 1546.101(a), (b), or (e) of this chapter, or an indirect air carrier, accepts it must be a SIDA. This includes areas such as: Cargo facilities; loading and unloading vehicle docks; and areas where an aircraft operator, foreign air carrier, or indirect air carrier sorts, stores, stages, consolidates, processes, screens, or transfers cargo.

(4) Other areas of the airport may be SIDAs.

(b) * * *

(2) Subject each individual to a criminal history records check as described in § 1542.209 before authorizing unescorted access to the SIDA.

* * * * *

(c) An airport operator that is not required to have a complete program under § 1542.103(a) is not required to establish a SIDA under this section.

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

■ 12. 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.

■ 13. Amend § 1544.3 by revising paragraph (c) to read as follows:

§ 1544.3 TSA inspection authority.

* * * * *

(c) TSA may enter and be present within secured areas, AOAs, SIDAs, and other areas where security measures required by TSA are carried out, without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

* * * * *

■ 14. Amend § 1544.101 by revising paragraphs (d)(1), (d)(4), and (e)(1), and adding new paragraphs (h) and (i) to read as follows:

§ 1544.101 Adoption and implementation.

* * * * *

(d) * * *

(1) Is an aircraft with a maximum certificated takeoff weight of more than 12,500 pounds;

* * * * *

(4) Is not under a full program, partial program, or full all-cargo program under paragraph (a), (b), or (h) of this section.

(e) * * *

(1) The requirements of §§ 1544.215, 1544.217, 1544.219, 1544.223, 1544.230, 1544.235, 1544.237, 1544.301(a) and (b), 1544.303, and 1544.305; and in addition, for all-cargo operations of §§ 1544.202, 1544.205(a), (b), (d), and (f).

* * * * *

(h) *Full all-cargo program—adoption:* Each aircraft operator must carry out the requirements of paragraph (i) of this section for each operation that is—

(1) In an aircraft with a maximum certificated takeoff weight of more than 45,500 kg (100,309.3 pounds); and

(2) Carrying cargo and authorized persons and no passengers.

(i) *Full all-cargo program—contents:* For each operation described in paragraph (h) of this section, the aircraft operator must carry out the following, and must adopt and carry out a security program that meets the applicable requirements of § 1544.103(c):

(1) The requirements of §§ 1544.202, 1544.205, 1544.207, 1544.209, 1544.211, 1544.215, 1544.217, 1544.219, 1544.225, 1544.227, 1544.228, 1544.229, 1544.230, 1544.231, 1544.233, 1544.235, 1544.237, 1544.301, 1544.303, and 1544.305.

(2) Other provisions of subpart C of this part that TSA has approved upon request.

(3) The remaining requirements of subpart C of this part when TSA notifies the aircraft operator in writing that a security threat exists concerning that operation.

■ 15. Add a new § 1544.202 to read as follows:

§ 1544.202 Persons and property onboard an all-cargo aircraft.

Each aircraft operator operating under a full all-cargo program, or a twelve-five program in an all-cargo operation, must apply the security measures in its security program for persons who board the aircraft for transportation, and for their property, to prevent or deter the carriage of any unauthorized persons, and any unauthorized weapons, explosives, incendiaries, and other destructive devices, items, or substances.

■ 16. Revise § 1544.205 to read as follows:

§ 1544.205 Acceptance and screening of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each aircraft operator operating under a full program, a full all-cargo program, or a twelve-five program in an all-cargo operation, must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized persons, and any unauthorized explosives, incendiaries, and other destructive substances or items in cargo onboard an aircraft.

(b) *Screening and inspection of cargo.* Each aircraft operator operating under a full program or a full all-cargo program, or a twelve-five program in an all-cargo operation, must ensure that cargo is screened and inspected for any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item as provided in the aircraft operator's security program and § 1544.207, and as provided in § 1544.239 for operations under a full program, before loading it on its aircraft.

(c) *Control.* Each aircraft operator operating under a full program or a full all-cargo program must use the procedures in its security program to control cargo that it accepts for transport on an aircraft in a manner that:

(1) Prevents the carriage of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item in cargo onboard an aircraft.

(2) Prevents unescorted access by persons other than an authorized aircraft operator employee or agent, or persons authorized by the airport operator or host government.

(d) *Refusal to transport.* Except as otherwise provided in its program, each aircraft operator operating under a full program, a full all-cargo program, or a twelve-five program in an all-cargo operation, must refuse to transport any cargo if the shipper does not consent to a search or inspection of that cargo in accordance with the system prescribed by this part.

(e) *Acceptance of cargo only from specified persons.* Each aircraft operator operating under a full program or a full all-cargo program may accept cargo for air transportation only from the shipper, or from an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program, as provided in its security program.

(f) *Acceptance and screening of cargo outside the United States.* For cargo to be loaded on its aircraft outside the United States, each aircraft operator must carry out the requirements of its security program.

■ 17. Amend § 1544.217 by revising paragraphs (a)(2) introductory text and (b) introductory text to read as follows:

§ 1544.217 Law enforcement personnel.

(a) * * *

(2) For operations under a partial program under § 1544.101(b) and (c), a twelve-five program under § 1544.101(d) and (e), a private charter program under § 1544.101(f), or a full all-cargo program under § 1544.101(h) and (i), each aircraft operator must—

* * * * *

(b) The following applies to operations at airports required to hold security programs under part 1542 of this chapter. For operations under a partial program under § 1544.101(b) and (c), a twelve-five program under § 1544.101(d) and (e), a private charter program under § 1544.101(f), or a full all-cargo program under § 1544.101(h) and (i), each aircraft operator must—

* * * * *

■ 18. Amend § 1544.225 by adding new paragraph (d) to read as follows:

§ 1544.225 Security of aircraft and facilities.

* * * * *

(d) When operating under a full program or a full all-cargo program, prevent unauthorized access to the operational area of the aircraft while loading or unloading cargo.

■ 19. Add a new § 1544.228 to read as follows:

§ 1544.228 Access to cargo: Security threat assessments for cargo personnel in the United States.

This section applies in the United States to each aircraft operator operating under a full program under § 1544.101(a), or a full all-cargo program under § 1544.101(h) of this part.

(a) This section applies for each employee and agent the aircraft operator authorizes to have unescorted access to cargo from the time—

(1) The cargo reaches a location where an aircraft operator with a full all-cargo program consolidates or inspects it pursuant to security program requirements until the cargo enters an airport Security Identification Display Area or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier; or

(2) An aircraft operator with a full program accepts the cargo until the cargo:

(i) Enters an airport Security Identification Display Area;

(ii) Is removed from the destination airport; or

(iii) Is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier.

(b) Before an aircraft operator authorizes, and before an employee or agent gains, unescorted access to cargo as described in paragraph (a) of this section, each employee or agent must successfully complete one of the following:

(1) A criminal history records check under §§ 1542.209, 1544.229, or 1544.230 of this chapter, if the employee or agent is otherwise required to undergo that check.

(2) A Security Threat Assessment under part 1540 subpart C of this chapter. An employee or agent who has successfully completed this Security Threat Assessment for one employer need not complete it for another employer if the employee or agent has been continuously employed in a position that requires a Security Threat Assessment.

(3) Another Security Threat Assessment approved by TSA as comparable to paragraphs (b)(1) or (2) of this section.

(c) Each aircraft operator must ensure that each individual who has access to its cargo—

(1) Has successfully completed one of the checks in paragraph (b) of this section;

(2) Is escorted by an employee or agent who has successfully completed one of the checks in paragraph (b) of this section; or

(3) Is authorized to serve as law enforcement personnel at that location.

(d) Operators must comply with the requirements of this section not later than November 22, 2006.

■ 20. Amend § 1544.229 by adding introductory text, and revising paragraph (a)(1)(iii) to read as follows:

§ 1544.229 Fingerprint-based criminal history records checks (CHRC): Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions.

This section applies to each aircraft operator operating under a full program, a private charter program, or a full all-cargo program.

(a) * * *

(1) * * *

(iii) Each individual granted authority to perform the following screening functions at locations within the United States (referred to as ''authority to perform screening functions''):

(A) Screening passengers or property that will be carried in a cabin of an aircraft of an aircraft operator required to screen passengers under this part.

(B) Serving as an immediate supervisor (checkpoint security supervisor (CSS)), and the next supervisory level (shift or site supervisor), to those individuals described in paragraphs (a)(1)(iii)(A) or (a)(1)(iii)(C) of this section.

(C) Screening cargo that will be carried on an aircraft of an aircraft operator with a full all-cargo program.

* * * * *

■ 21. Add a new § 1544.239 to read as follows:

§ 1544.239 Known shipper program.

This section applies to each aircraft operator operating under a full program under § 1544.101(a) of this part and to each aircraft operator with a TSA security program approved for transfer of cargo to an aircraft operator with a full program or a foreign air carrier under paragraphs § 1546.101(a) or (b) of this chapter.

(a) For cargo to be loaded on its aircraft in the United States, each aircraft operator must have and carry out a known shipper program in accordance with its security program. The program must—

(1) Determine the shipper's validity and integrity as provided in the security program;

(2) Provide that the aircraft operator will separate known shipper cargo from unknown shipper cargo; and

(3) Provide for the aircraft operator to ensure that cargo is screened or inspected as set forth in its security program.

(b) When required by TSA, each aircraft operator must submit in a form and manner acceptable to TSA—

(1) Information identified in its security program regarding a known shipper, or an applicant for that status; and

(2) Corrections and updates of this information upon learning of a change to the information specified in paragraph (b)(1) of this section.

PART 1546—FOREIGN AIR CARRIER SECURITY

■ 22. 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.

■ 23. Amend § 1546.3 by adding new paragraph (c) to read as follows:

§ 1546.3 TSA inspection authority.

* * * * *

(c) TSA may enter and be present within secured areas, AOAs, SIDAs, and other areas where security measures required by TSA are carried out, without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

■ 24. Amend § 1546.101 by revising the introductory text and paragraph (a), and by adding new paragraphs (e) and (f) to read as follows:

§ 1546.101 Adoption and implementation.

Each foreign air carrier landing or taking off in the United States must adopt and carry out, for each scheduled and public charter passenger operation or all-cargo operation, a security program that meets the requirements of—

(a) Section 1546.103(b) and subparts C, D, and E of this part for each operation with an aircraft having a passenger seating configuration of 61 or more seats;

* * * * *

(e) Sections 1546.103(b)(2) and (b)(4), 1546.202, 1546.205(a), (b), (c), (d), (e), and (f), 1546.207, 1546.211, 1546.213, and 1546.301 for each all-cargo operation with an aircraft having a maximum certificated take-off weight more than 45,500 kg (100,309.3 lbs.); and

(f) Sections 1546.103(b)(2) and (b)(4), 1546.202, 1546.205(a), (b), (d), and (f), 1546.211, and 1546.301 for each all-cargo operation with an aircraft having a maximum certificated take-off weight more than 12,500 pounds but not more than 45,500 kg (100,309.3 lbs.).

■ 25. Amend § 1546.103 by revising paragraph (a)(1) and paragraph (b) introductory text to read as follows:

§ 1546.103 Form, content, and availability of security program.

(a) * * *

(1) *Acceptable to TSA.* A foreign air carrier's security program is acceptable only if TSA finds that the security program provides a level of protection similar to the level of protection provided by U.S. aircraft operators serving the same airports. Foreign air carriers must employ procedures equivalent to those required of U.S. aircraft operators serving the same airport, if TSA determines that such procedures are necessary to provide a similar level of protection.

* * * * *

(b) *Content of security program.* Each security program required by § 1546.101(a), (b), (c), (e), or (f) must be designed to—

* * * * *

■ 26. Add a new § 1546.202 to read as follows:

§ 1546.202 Persons and property onboard the aircraft.

Each foreign air carrier operating under § 1546.101(e) or (f) must apply the security measures in its security program for persons who board the aircraft for transportation, and for their property, to prevent or deter the carriage of any unauthorized persons, and any unauthorized weapons, explosives, incendiaries, and other destructive devices, items, or substances.

■ 27. Revise § 1546.205 to read as follows:

§ 1546.205 Acceptance and screening of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each foreign air carrier operating a program under § 1546.101(a), (b), (e), or (f) must use the procedures, facilities, and equipment described in its security program to prevent or deter the carriage of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item in cargo onboard an aircraft.

(b) *Refusal to transport.* Each foreign air carrier operating a program under § 1546.101(a), (b), (e), or (f) must refuse to transport any cargo, if the shipper does not consent to a search or inspection of that cargo in accordance with the system prescribed by this part.

(c) *Control.* Each foreign air carrier operating a program under § 1546.101(a), (b), or (e) must use the procedures in its security program to control cargo that it accepts for transport on an aircraft in a manner that—

(1) Prevents the carriage of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item onboard the aircraft.

(2) Prevents access by unauthorized persons other than an authorized foreign air carrier employee or agent, or persons authorized by the airport operator or host government.

(d) *Screening and inspection of cargo in the United States.* Each foreign air carrier operating a program under § 1546.101(a), (b), (e), or (f) must ensure that, as required in its security program, cargo is screened and inspected for any unauthorized persons, and any unauthorized explosives, incendiaries, and other destructive substances or items as provided in the foreign air carrier's security program, and § 1546.207, and as provided in § 1546.213 for operations under § 1546.101(a) or (b) before loading it on its aircraft in the United States.

(e) *Acceptance of cargo in the United States only from specified persons.* Each foreign air carrier operating a program under § 1546.101(a), (b), or (e) of this part may accept cargo in the United States only from the shipper, or from an aircraft operator, foreign air carrier, or indirect air carrier operating under a security program under this chapter with a comparable cargo security program as provided in its security program.

(f) *Acceptance of cargo to be loaded for transport to the United States.* Each foreign air carrier subject to this part that accepts cargo to be loaded on its aircraft for transport to the United States must carry out the requirements of its security program.

■ 28. Add a new § 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) This section applies to each employee or agent in the United States whom the foreign air carrier authorizes to have unescorted access to cargo from the time—

(1) The cargo reaches a location where a foreign air carrier operating under § 1546.101(e) consolidates or inspects it pursuant to security program requirements, until the cargo enters an airport Security Identification Display Area or is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier, or

(2) A foreign air carrier under § 1546.101(a) or (b) accepts the cargo, until the cargo—

(i) Enters an airport Security Identification Display Area;

(ii) Is removed from the destination airport; or

(iii) Is transferred to another TSA-regulated aircraft operator, foreign air carrier, or indirect air carrier.

(b) Before a foreign air carrier authorizes, and before an employee or agent gains, unescorted access to cargo as described in paragraph (a) of this section, each employee or agent must successfully complete one of the following:

(1) A criminal history records check under §§ 1542.209, 1544.229, or 1544.230 of this chapter, if the employee or agent is otherwise required to undergo that check.

(2) A Security Threat Assessment under part 1540 subpart C of this chapter. An employee or agent who has successfully completed this Security Threat Assessment for one employer need not complete it for another employer, if the employee or agent has been continuously employed in a position that requires a Security Threat Assessment.

(3) Another Security Threat Assessment approved by TSA as comparable to paragraphs (b)(1) or (2) of this section.

(c) Each foreign air carrier must ensure that each individual who has access to its cargo—

(1) Has successfully completed one of the checks in paragraph (b) of this section;

(2) Is escorted by an employee or agent who has successfully completed one of the checks in paragraph (b) of this section; or

(3) Is authorized to serve as law enforcement personnel at that location.

(d) Operators must comply with the requirements of this section not later than November 22, 2006.

■ 29. Add a new § 1546.215 to read as follows:

§ 1546.215 Known shipper program.

This section applies to each foreign air carrier operating a program under § 1546.101(a) or (b).

(a) For cargo to be loaded on its aircraft in the United States, each foreign air carrier must have and carry out a known shipper program in accordance with its security program. The program must—

(1) Determine the shipper's validity and integrity as provided in the foreign air carrier's security program;

(2) Provide that the foreign air carrier will separate known shipper cargo from unknown shipper cargo; and

(3) Provide for the foreign air carrier to ensure that cargo is screened or inspected as set forth in its security program.

(b) When required by TSA, each foreign air carrier must submit in a form and manner acceptable to TSA—

(1) Information identified in its security program regarding an applicant to be a known shipper or a known shipper; and

(2) Corrections and updates to the information upon learning of a change to the information specified in paragraph (b)(1) of this section.

■ 30. Amend § 1546.301 by revising the introductory text to read as follows:

§ 1546.301 Bomb or air piracy threats.

No foreign air carrier may land or take off an airplane in the United States after receiving a bomb or air piracy threat against that airplane, unless the following actions are taken:

* * * * *

PART 1548—INDIRECT AIR CARRIER SECURITY

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

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

■ 32. Amend § 1548.3 by adding new paragraph (c) to read as follows:

§ 1548.3 TSA inspection authority.

* * * * *

(c) TSA may enter and be present within areas where security measures required by TSA are carried out without access media or identification media issued or approved by the indirect air carrier, an airport operator, or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

■ 33. Amend § 1548.5 by revising paragraphs (a), (b), and (c) to read as follows:

§ 1548.5 Adoption and implementation of the security program.

(a) *Security program required.* No indirect air carrier may offer cargo to an aircraft operator operating under a full program or a full all-cargo program specified in part 1544 of this subchapter, or to a foreign air carrier operating under a program under § 1546.101(a), (b), or (e) of this subchapter, unless that indirect air carrier has and carries out an approved security program under this part. Each indirect air carrier that does not currently hold a security program under part 1548, and that offers cargo to an aircraft operator operating under a full all-cargo program or a comparable operation by a foreign air carrier must comply with this section not later than November 22, 2006.

(b) *General requirements.* (1) The security program must provide for the security of the aircraft, as well as that of persons and property traveling in air transportation against acts of criminal violence and air piracy and against the introduction into the aircraft of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item as provided in the indirect air carrier's security program. This requirement applies—

(i) From the time the indirect air carrier accepts the cargo to the time it transfers the cargo to an entity that is not an employee or agent of the indirect air carrier;

(ii) While the cargo is stored, en route, or otherwise being handled by an employee or agent of the indirect air carrier; and

(iii) Regardless of whether the indirect air carrier has or ever had physical possession of the cargo.

(2) The indirect air carrier must ensure that its employees and agents carry out the requirements of this chapter and the indirect air carrier's security program.

(c) *Content.* Each security program under this part must—

(1) Be designed to prevent or deter the introduction of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item onto an aircraft.

(2) Include the procedures and description of the facilities and equipment used to comply with the requirements of §§ 1548.9 and 1548.17 regarding the acceptance and offering of cargo.

(3) Include the procedures and syllabi used to accomplish the training required under § 1548.11 of persons who accept, handle, transport, or deliver cargo on behalf of the indirect air carrier.

* * * * *

■ 34. Revise § 1548.7 to read as follows:

§ 1548.7 Approval, amendment, annual renewal, and withdrawal of approval of the security program.

(a) *Original Application*—(1) *Application.* The applicant must apply for a security program in a form and a manner prescribed by TSA not less than 90 calendar days before the applicant intends to begin operations. The application must be in writing and include:

(i) The business name; other names, including doing business as; state of incorporation, if applicable; and tax identification number.

(ii) The applicant names, addresses, and dates of birth of each proprietor, general partner, officer, director, and owner identified under § 1548.16.

(iii) A signed statement from each person listed in paragraph (a)(1)(ii) of this section stating whether he or she has been a proprietor, general partner, officer, director, or owner of an IAC that had its security program withdrawn by TSA.

(iv) Copies of government-issued identification of persons listed in paragraph (a)(1)(ii) of this section.

(v) Addresses of all business locations in the United States.

(vi) A statement declaring whether the business is a "'small business'" pursuant to section 3 of the Small Business Act (15 U.S.C. 632).

(vii) A statement acknowledging and ensuring that each employee and agent of the indirect air carrier, who is subject to training under § 1548.11, will have successfully completed the training outlined in its security program before performing security-related duties.

(viii) Other information requested by TSA concerning Security Threat Assessments.

(ix) A statement acknowledging and ensuring that each employee and agent will successfully complete a Security Threat Assessment under § 1548.15 before authorizing the individual to have unescorted access to cargo.

(2) *Approval.* TSA will approve the security program by providing the indirect air carrier with the Indirect Air Carrier Standard Security Program and any Security Directive upon determining that—

(i) The indirect air carrier has met the requirements of this part, its security program, and any applicable Security Directive;

(ii) The approval of its security program is not contrary to the interests of security and the public interest; and

(iii) The indirect air carrier has not held a security program that was withdrawn within the previous year, unless otherwise authorized by TSA.

(3) *Commencement of operations.* The indirect air carrier may operate under a security program when it meets all requirements, including but not limited to successful completion of training and Security Threat Assessments by relevant personnel.

(4) *Duration of security program.* The security program will remain effective until the end of the calendar month one year after the month it was approved.

(5) *Requirement to report changes in information.* Each indirect air carrier with an approved security program under this part must notify TSA, in a form and manner approved by TSA, of any changes to the information submitted during its initial application.

(i) This notification must be submitted to the designated official not later than 30 days after the date the change occurred.

(ii) Changes included in the requirement of this paragraph include, but are not limited to, changes in the indirect air carrier's contact information, owners, business addresses and locations, and form of business entity.

(b) *Renewal Application.* Upon timely submittal of an application for renewal, and unless and until TSA denies the application, the indirect air carrier's approved security program remains in effect.

(1) Unless otherwise authorized by TSA, each indirect air carrier that has a security program under this part must timely submit to TSA, at least 30 calendar days prior to the first day of the anniversary month of initial approval of its security program, an application for renewal of its security program in a form and a manner approved by TSA.

(2) The application for renewal must be in writing and include a signed statement that the indirect air carrier has reviewed and ensures the continuing accuracy of the contents of its initial application for a security program, subsequent renewal applications, or other submissions to TSA confirming a change of information and noting the date such applications and submissions were sent to TSA, including the following certification:

[Name of indirect air carrier] (hereinafter ''the IAC'') has adopted and is currently carrying out a security program in accordance with the Transportation Security Regulations as originally approved on [Insert date of TSA initial approval]. In accordance with TSA regulations, the IAC has notified TSA of any new or changed information required for the IAC's initial security program. If new or changed information is being submitted to TSA as part of this application for reapproval, that information is stated in this filing.

The IAC understands that intentional falsification of certification to an air carrier or to TSA may be subject to both civil and criminal penalties under 49 CFR 1540 and 1548 and 18 U.S.C. 1001. Failure to notify TSA of any new or changed information required for initial approval of the IAC's security program in a timely fashion and in a form acceptable to TSA may result in withdrawal by TSA of approval of the IAC's security program.

(3) TSA will renew approval of the security program if TSA determines that—

(i) The indirect air carrier has met the requirements of this chapter, its security program, and any Security Directive; and

(ii) The renewal of its security program is not contrary to the interests of security and the public interest.

(4) If TSA determines that the indirect air carrier meets the requirements of paragraph (b)(3) of this section, it will renew the indirect air carrier's security program. The security program will remain effective until the end of the calendar month one year after the month it was renewed.

(c) *Amendment requested by an indirect air carrier or applicant.* An indirect air carrier or applicant may file a request for an amendment to its security program with the TSA designated official at least 45 calendar days before the date it proposes for the amendment to become effective, unless the designated official allows a shorter period. Any indirect air carrier may submit a group proposal for an amendment that is on behalf of it and other indirect air carriers that co-sign the proposal.

(1) Within 30 calendar days after receiving a proposed amendment, the designated official, in writing, either approves or denies the request to amend.

(2) An amendment to an indirect air carrier security program may be approved, if the designated official determines that safety and the public interest will allow it, and if the proposed amendment provides the level of security required under this part.

(3) Within 30 calendar days after receiving a denial of the proposed amendment, the indirect air carrier may petition TSA to reconsider the denial. A petition for reconsideration must be filed with the designated official.

(4) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to the TSA for reconsideration. TSA will dispose of the petition within 30 calendar days of receipt by either directing the designated official to approve the amendment or by affirming the denial.

(d) *Amendment by TSA.* TSA may amend a security program in the interest of safety and the public interest, as follows:

(1) TSA notifies the indirect air carrier, in writing, of the proposed amendment, fixing a period of not less than 30 calendar days within which the indirect air carrier may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the designated official notifies the indirect air carrier of any amendment adopted or rescinds the notice of amendment. If the amendment is adopted, it becomes effective not less than 30 calendar days after the indirect air carrier receives the notice of amendment, unless the indirect air carrier disagrees with the proposed amendment and petitions the TSA to reconsider, no later than 15 calendar days before the effective date of the amendment. The indirect air carrier must send the petition for reconsideration to the designated official. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the designated official either amends or withdraws the notice of amendment, or transmits the petition, together with any pertinent information, to TSA for reconsideration. TSA disposes of the petition within 30 calendar days of receipt, either by directing the designated official to withdraw or amend the notice of amendment, or by affirming the notice of amendment.

(e) *Emergency Amendments.* (1) If TSA finds that there is an emergency requiring immediate action, with respect to aviation security that makes procedures in this section contrary to the public interest, the designated official may issue an emergency amendment, without the prior notice and comment procedures described in paragraph (d) of this section.

(2) The emergency amendment is effective without stay on the date the indirect air carrier receives notification. TSA will incorporate in the notification a brief statement of the reasons and findings for the emergency amendment to be adopted.

(3) The indirect air carrier may file a petition for reconsideration with the TSA no later than 15 calendar days after TSA issued the emergency amendment. The indirect air carrier must send the petition for reconsideration to the designated official; however, the filing does not stay the effective date of the emergency amendment.

(f) *Withdrawal of approval of a security program.* TSA may withdraw the approval of the indirect air carrier's security program, if TSA determines

continued operation is contrary to safety and the public interest, as follows:

(1) *Notice of proposed withdrawal of approval.* The designated official will serve a notice of proposed withdrawal of approval, which notifies the indirect air carrier, in writing, of the facts, charges, and applicable law, regulation, or order that form the basis for the determination.

(2) *Indirect air carrier reply.* The indirect air carrier may respond to the notice of proposed withdrawal of approval no later than 15 calendar days after receipt of the withdrawal by providing the designated official, in writing, with any material facts, arguments, applicable law, and regulation.

(3) *TSA review.* The designated official will consider all information available, including any relevant material or information submitted by the indirect air carrier, before either issuing a withdrawal of approval of the indirect air carrier's security program or rescinding the notice of proposed withdrawal of approval. If TSA issues a withdrawal of approval, it becomes effective upon receipt by the indirect air carrier, or 15 calendar days after service, whichever occurs first.

(4) *Petition for reconsideration.* The indirect air carrier may petition the TSA to reconsider the withdrawal of approval by serving a petition for consideration no later than 15 calendar days after the indirect air carrier receives the withdrawal of approval. The indirect air carrier must serve the petition for reconsideration on the designated official. Submission of a petition for reconsideration will not automatically stay the withdrawal of approval. The indirect air carrier may request the designated official to stay the withdrawal of approval pending consideration of the petition.

(5) *Assistant Secretary's review.* The designated official transmits the petition together with all pertinent information to the Assistant Secretary for reconsideration. The Assistant Secretary will dispose of the petition within 15 calendar days of receipt by either directing the designated official to rescind the withdrawal of approval or by affirming the withdrawal of approval. The decision of the Assistant Secretary is a final order subject to judicial review in accordance with 49 U.S.C. 46110.

(6) *Emergency withdrawal.* If TSA finds that there is an emergency requiring immediate action, with respect to aviation security that makes procedures in this section contrary to the public interest, the designated official may issue an emergency withdrawal of the indirect air carrier's security program, without first issuing a notice of proposed withdrawal, effective without stay on the date that the indirect air carrier receives notice of the emergency withdrawal. In such a case, the designated official will send the indirect air carrier a brief statement of the facts, charges, and applicable law, regulation, or order that forms the basis for the emergency withdrawal. The indirect air carrier may submit a petition for reconsideration under the procedures in paragraphs (f)(2) through (f)(5) of this section; however, this petition will not stay the effective date of the emergency withdrawal.

(g) *Service of documents for withdrawal of approval of security program proceedings.* Service may be accomplished by personal delivery, certified mail, or express courier. Documents served on an indirect air carrier will be served at the indirect air carrier's official place of business as designated in its application for approval or its security program. Documents served on TSA must be served to the address noted in the notice of withdrawal of approval or withdrawal of approval, whichever is applicable.

(1) *Certificate of service.* An individual may attach a certificate of service to a document tendered for filing. A certificate of service must consist of a statement, dated and signed by the person filing the document, that the document was personally delivered, served by certified mail on a specific date, or served by express courier on a specific date.

(2) *Date of service.* The date of service will be—

(i) The date of personal delivery;

(ii) If served by certified mail, the mailing date shown on the certificate of service, the date shown on the postmark, if there is no certificate of service, or other mailing date shown by other evidence if there is no certificate of service or postmark; or

(iii) If served by express courier, the service date shown on the certificate of service, or by other evidence if there is no certificate of service.

(h) *Extension of time.* TSA may grant an extension of time of the limits set forth in this section for good cause shown. An indirect air carrier's request for an extension of time must be in writing and be received by TSA at least 2 days before the due date to be extended. TSA may grant itself an extension of time for good cause.

■ 35. Revise § 1548.9 to read as follows:

§ 1548.9 Acceptance of cargo.

(a) *Preventing or deterring the carriage of any explosive or incendiary.* Each indirect air carrier must use the facilities, equipment, and procedures described in its security program to prevent or deter the carriage onboard an aircraft of any unauthorized person, and any unauthorized explosive, incendiary, and other destructive substance or item, as provided in the indirect air carrier's security program.

(b) *Refusal to transport.* Each indirect air carrier must refuse to offer for transport on an aircraft any cargo, if the shipper does not consent to a search or inspection of that cargo in accordance with this part, or parts 1544 or 1546 of this chapter.

■ 36. Add a new § 1548.11 to read as follows:

§ 1548.11 Training and knowledge for individuals with security-related duties.

(a) No indirect air carrier may use an employee or agent to perform any security-related duties to meet the requirements of its security program, unless that individual has received training, as specified in its security program, including his or her personal responsibilities in § 1540.105 of this chapter.

(b) Each indirect air carrier must ensure that each of its authorized employees or agents who accept, handle, transport, or deliver cargo have knowledge of the—

(1) Applicable provisions of this part;

(2) Applicable Security Directives and Information Circulars;

(3) The approved airport security program(s) applicable to their location(s); and

(4) The aircraft operator's or indirect air carrier's security program, to the extent necessary in order to perform their duties.

(c) Each indirect air carrier must ensure that each of its authorized employees or agents under paragraph (b) of this section successfully completes recurrent training at least annually on their individual responsibilities in—

(1) Section 1540.105 of this chapter;

(2) The applicable provisions of this part;

(3) Applicable Security Directives and Information Circulars;

(4) The approved airport security program(s) applicable to their location(s); and

(5) The aircraft operator's or indirect air carrier's security program, to the extent that such individuals need to know in order to perform their duties.

(d) Operators must comply with the requirements of this section by November 22, 2006.

■ 37. Add a new § 1548.13 to read as follows:

§ 1548.13 Security coordinators.

Each indirect air carrier must designate and use an Indirect Air Carrier Security Coordinator (IACSC). The IACSC and alternates must be appointed at the corporate level and must serve as the indirect air carrier's primary contact for security-related activities and communications with TSA, as set forth in the security program. Either the IACSC or an alternate IACSC must be available on a 24-hour basis.

■ 38. Add a new § 1548.15 to read as follows:

§ 1548.15 Access to Cargo: Security threat assessments for individuals having unescorted access to cargo.

This section applies to each indirect air carrier operating under this part.

(a) This section applies to each employee or agent the indirect air carrier authorizes to have unescorted access to cargo from the time—

(1) Cargo to be transported on an aircraft operated by an aircraft operator with a full all-cargo program under § 1544.101(h) of this chapter, or by a foreign air carrier under § 1546.101(e) of this chapter, reaches an indirect air carrier facility where the indirect air carrier consolidates or holds the cargo until the indirect air carrier transfers the cargo to an aircraft operator or foreign air carrier, or

(2) Cargo to be transported on an aircraft operated by an aircraft operator with a full program or by a foreign air carrier under § 1546.101(a) or (b) of this chapter, is accepted by the indirect air carrier.

(b) Before an indirect air carrier authorizes, and before an employee or agent gains, unescorted access to cargo as described in paragraph (a) of this section, each employee or agent must successfully complete one of the following:

(1) A criminal history records check under §§ 1542.209, 1544.229, or 1544.230 of this chapter, if the individual is otherwise required to undergo that check.

(2) A Security Threat Assessment under part 1540 subpart C of this chapter. An employee or agent who has successfully completed this Security Threat Assessment for one employer need not complete it for another employer if the employee or agent has been continuously employed in a position that requires a Security Threat Assessment.

(3) Another Security Threat Assessment approved by TSA as comparable to paragraphs (b)(1) or (b)(2) of this section.

(c) Each indirect air carrier must ensure that each individual who has access to its cargo—

(1) Has successfully completed one of the checks in paragraph (b) of this section;

(2) Is escorted by a person who has successfully completed one of the checks in paragraph (b) of this section; or

(3) Is authorized to serve as law enforcement personnel at that location.

(d) Operators must comply with the requirements of this section not later than November 22, 2006.

■ 39. Add a new § 1548.16 to read as follows:

§ 1548.16 Security threat assessments for each proprietor, general partner, officer, director, and certain owners of the entity.

(a) Each indirect air carrier, or applicant to be an indirect air carrier, must ensure that each proprietor, general partner, officer, director, and owner of the entity has successfully completed a Security Threat Assessment under part 1540 subpart C of this chapter. Each indirect air carrier must comply with the requirements of this section not later than November 22, 2006.

(b) For purposes of this section, *owner* means—

(1) A person who directly or indirectly owns, controls, or has power to vote 25 percent or more of any class of voting securities or other voting interests of an IAC or applicant to be an IAC; or

(2) A person who directly or indirectly controls in any manner the election of a majority of the directors (or individuals exercising similar functions) of an IAC, or applicant to be an IAC.

(c) For purposes of this definition of *owner*—

(1) Members of the same family must be considered to be one person.

(i) *Same family* means parents, spouses, children, siblings, uncles, aunts, grandparents, grandchildren, first cousins, stepchildren, stepsiblings, and parents-in-law, and spouses of any of the foregoing.

(ii) Each member of the same family, who has an ownership interest in an IAC, or an applicant to be an IAC, must be identified if the family is an owner as a result of aggregating the ownership interests of the members of the family.

(iii) In determining the ownership of interests of the same family, any voting interest of any family member must be taken into account.

(2) *Voting securities or other voting interests* means securities or other interests that entitle the holder to vote for or select directors (or individuals exercising similar functions).

■ 40. Add a new § 1548.17 to read as follows:

§ 1548.17 Known shipper program.

This section applies to cargo that an indirect air carrier offers to an aircraft operator operating under a full program under § 1544.101(a) of this chapter, or to a foreign air carrier operating under § 1546.101(a) or (b) of this chapter.

(a) For cargo to be loaded on aircraft in the United States, each indirect air carrier must have and carry out a known shipper program in accordance with its security program. The program must—

(1) Determine the shipper's validity and integrity as provided in its security program;

(2) Provide that the indirect air carrier will separate known shipper cargo from unknown shipper cargo.

(b) When required by TSA, each indirect air carrier must submit to TSA, in a form and manner acceptable to TSA—

(1) Information identified in its security program regarding an applicant to be a known shipper or a known shipper; and

(2) Corrections and updates of this information upon learning of a change to the information specified in paragraph (b)(1) of this section.

■ 41. Add a new § 1548.19 to read as follows:

§ 1548.19 Security Directives and Information Circulars.

(a) TSA may issue an Information Circular to notify indirect air carriers of security concerns.

(b) When TSA determines that additional security measures are necessary to respond to a threat assessment, or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(1) Each indirect air carrier that is required to have an approved indirect air carrier security program must comply with each Security Directive that TSA issues to it, within the time prescribed in the Security Directive for compliance.

(2) Each indirect air carrier that receives a Security Directive must comply with the following:

(i) Within the time prescribed in the Security Directive, acknowledge in writing receipt of the Security Directive to TSA.

(ii) Within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective).

(3) In the event that the indirect air carrier is unable to implement the

measures in the Security Directive, the indirect air carrier must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval.

(i) The indirect air carrier must submit the proposed alternative measures within the time prescribed in the Security Directive.

(ii) The indirect air carrier must implement any alternative measures approved by TSA.

(4) Each indirect air carrier that receives a Security Directive may comment on it by submitting data, views, or arguments in writing to TSA.

(i) TSA may amend the Security Directive based on comments received.

(ii) Submission of a comment does not delay the effective date of the Security Directive.

(5) Each indirect air carrier that receives a Security Directive or Information Circular, and each person who receives information from a Security Directive or Information Circular, must:

(i) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with a need-to-know.

(ii) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those with a need-to-know without the prior written consent of TSA.

Issued in Arlington, Virginia, on May 17, 2006.

Kip Hawley,

Assistant Secretary.

[FR Doc. 06–4800 Filed 5–25–06; 8:45 am]

BILLING CODE 9110–05–P