DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

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

[Docket No. TSA–2004–19515]

RIN 1652–AA23

Air Cargo Security Requirements

AGENCY: Transportation Security Administration (TSA), Department of Homeland Security (DHS).

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The Transportation Security Administration (TSA), an agency within the Department of Homeland Security's Border and Transportation Security Directorate, proposes to amend current transportation security regulations to enhance and improve the security of air cargo transportation. The Aviation and Transportation Security Act directed TSA to implement measures to enhance the security of air cargo transported in both passenger and all-cargo aircraft. In discharging this responsibility, TSA conducted analyses of internal and external threats, risk and vulnerability assessments, and security measures already in place. This proposed rulemaking would require the adoption of security measures throughout the air cargo supply chain; these security measures will be applicable to airport operators, aircraft operators, foreign air carriers, and indirect air carriers. These proposed regulatory requirements would impose significant barriers to terrorists seeking to use the air cargo transportation system for malicious purposes.

This proposal would also change the applicability of the requirement for a ''twelve-five'' security program from aircraft with a maximum certificated takeoff weight ''of 12,500 pounds or more'' to those with a maximum certificated takeoff weight of ''more than 12,500 pounds.'' This change would conform the regulation to recent legislation.

DATES: Send your comments on or before January 10, 2005.

ADDRESSES: You may submit comments, identified by the TSA docket number, to this rulemaking using any one of the following methods:

Comments Filed Electronically: You may submit comments through the docket Web site at *http://dms.dot.gov.* Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the applicable Privacy Act Statement published in the **Federal Register** on April 11, 2000 (65 FR 19477), or you may visit *http://dms.dot.gov.*

You also may submit comments through the Federal eRulemaking portal at *http://www.regulations.gov.*

Comments Submitted by Mail, Fax, or In Person: Address or deliver your written, signed comments to the Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590–0001; Fax: 202–493–2251.

Comments that include trade secrets, confidential commercial or financial information, or sensitive security information (SSI) should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the proposed rule. Comments containing trade secrets, confidential commercial or financial information, or SSI should be appropriately marked as containing such information and submitted by mail to the individual listed in **FOR FURTHER INFORMATION CONTACT**.

Reviewing Comments in the Docket: You may review the public docket containing comments in person in the Dockets Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located on the plaza level of the NASSIF Building at the Department of Transportation address above. Also, you may review public dockets on the Internet at *http://dms.dot.gov*.

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

FOR FURTHER INFORMATION CONTACT: Tamika McCree, Transportation Security Administration, Office of Transportation Security Policy (TSA–9), 601 South 12th Street, Arlington, Virginia, 22202, (571–227–2632), *tamika.mccree@dhs.gov*.

SUPPLEMENTARY INFORMATION:

Comments Invited

The TSA invites interested persons to participate in this rulemaking by submitting written comments, data, or views. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from adopting the proposals in this document. See **ADDRESSES** above for information on where to submit comments.

With each comment, please include your name and address, identify the docket number at the beginning of your comments, and give the reason for each comment. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. You may submit comments and material electronically, in person, or by mail as provided under **ADDRESSES**, but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in two copies, in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

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

Except for comments containing confidential information and SSI, we will file in the public docket all comments we receive, as well as a report summarizing each substantive public contact with TSA personnel concerning this rulemaking. The docket is available for public inspection before and after the comment closing date.

We will consider all comments we receive on or before the closing date for comments. We will consider comments filed late to the extent practicable. We may change this rulemaking in light of the comments we receive.

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.access.gpo.gov/su_docs/aces/aces140.html*; or

(3) Visiting the TSA's Law and Policy web page at *http://www.tsa.dot.gov/public/index.jsp.*

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.

Abbreviations and Terms Used in This Document

ACSSP—Air Carrier Standard Security Program

ASAC—Aviation Security Advisory Committee

ATSA—Aviation and Transportation Security Act

CBP—U.S. Customs and Border Protection

C–TPAT—Customs-Trade Partnership Against Terrorism
DHS—Department of Homeland Security
DOT—Department of Transportation
DSIP—Domestic Security Integration Program
EA—Emergency Amendment
FAA—Federal Aviation Administration
IAC—Indirect Air Carrier
IACSSP—Indirect Air Carrier Standard Security Program
IC—Information Circular
SD—Security Directive
SIDA—Security Identification Display Area
SSI—Sensitive Security Information
TSA—Transportation Security Administration

Outline of Notice of Proposed Rulemaking:

I. Background

On September 11, 2001, terrorist attacks against the United States resulted in unprecedented human casualties and property damage. In response to those attacks, Congress passed the Aviation and Transportation Security Act (ATSA), which established the Transportation Security Administration. TSA was created as an agency within the Department of Transportation (DOT), operating under the direction of the Under Secretary of Transportation for Security. On March 1, 2003, TSA was transferred to the Department of Homeland Security (DHS);[1] the office formerly designated DOT Under Secretary for Transportation Security is now Administrator of TSA. TSA continues to have the statutory authority and responsibility that ATSA granted to the Administrator with respect to security in all modes of transportation.[2] In ATSA, Congress set forth the following specific requirements for TSA in the area of air cargo security:

- 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 an air carrier or foreign air carrier; [3] 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.[4]

TSA has addressed air cargo security through the issuance of regulations, Security Directives (SDs), and Emergency Amendments (EAs) to security programs. All cargo loaded on passenger aircraft is subject to security requirements through TSA's known shipper program, which prohibits operators of passenger aircraft from transporting any cargo from shippers that are unknown.[5] Notably, in 49 U.S.C. section 44901(a), Congress expressly provided that the known shipper program is a form of screening that need not be carried out by a Federal government employee, unlike most screening of persons and property that is loaded on a passenger aircraft. Thus, aircraft operators carry out screening using the known shipper program.

The known shipper program has been substantially strengthened since September 11, 2001, and additional security measures have been implemented over the last two years. TSA prohibits aircraft operators in passenger operations under full programs [6] from transporting cargo unless a Known Shipper ships it. Entities may qualify for Known Shipper status if they meet certain security requirements. This proposed rule would codify the known shipper program as well as provide enhancements to the existing structure to strengthen the program further.

This proposed rule also includes other elements to improve security of air cargo carried on passenger aircraft. With respect to all-cargo aircraft, this proposed rule would enhance security significantly by requiring the adoption of a number of measures by airports, aircraft operators, and indirect air carriers (IACs), sometimes known as air freight forwarders.

Following the acts of terrorism on September 11, the Federal Aviation Administration (FAA) and then the Transportation Security Administration (TSA) took steps to amend security regulations governing aviation security, including the acceptance and handling of air cargo. While other agencies, including FAA, regulate safety considerations in the transportation of cargo and U.S. Customs and Border Protection (CBP) regulates the entry of cargo into the United States, TSA is solely responsible for the security of shipments of air cargo. The requirements outlined in this proposed rule, including those presently implemented by security directives, would comprehensively enhance the security of air cargo. These proposals would fill gaps in existing air cargo security regulations to mitigate the threat of terrorism to this vital industry.

Section IV of this NPRM specifically addresses each of the changes made to 49 CFR parts 1540–1548 and discusses how those changes will improve air cargo security. The major objectives of the program are to prevent passenger and large all-cargo aircraft from being used as weapons and to prevent unauthorized explosives from being carried aboard, and potentially detonated, during flight. In summary, DHS is proposing to establish a Standard Security Program for all-cargo aircraft operators utilizing aircraft with a take-off weight of over 45,500 kg. These carriers currently are not covered by the requirement in section

[1] Homeland Security Act, Pub. L. 107–296 (Nov. 25, 2002).

[2] 49 U.S.C. 114(d).

[3] 49 U.S.C. 44901(a)

[4] 49 U.S.C. 44901(f)

[5] See discussion on Known Shipper Program at IV.G.

[6] See discussion of aircraft operator security programs in IV. of this preamble.

1544.101(a) as they relate to the cargo provisions of section 1544.205 because they do not carry passengers. Instead, these all-cargo operators typically follow provisions of 1544.101(d) and (e), which are intended to govern the operations of much smaller aircraft. The current rules for cargo carried on certain passenger aircraft, and for other all-cargo operations under the existing Twelve-Five Standard Security Program, would be enhanced. DHS also proposes to extend security threat assessments, or focused background checks, to air cargo industry workers who handle air cargo but do not operate within a secure area. Currently, these workers are not screened, leaving the possibility that they could introduce weapons, explosives, or individuals into the air cargo system. For similar reasons, we also propose to extend Secure Identification Display Area requirements at airports that have these areas under § 1544.205 to cargo operation areas not covered by the current language of this regulation. We also seek to ensure persons traveling on all-cargo aircraft are screened to ensure they do not pose a threat to the aircraft. Finally the draft regulation would bolster the requirements imposed on indirect air carriers in recognition of the fact that vulnerabilities within their operations could lead to the introduction of weapons, explosives, or individuals who may jeopardize the security of aircraft. None of these measures is currently covered under existing TSA or other agency regulations.

CBP has issued regulations governing international air cargo, but the CBP regulations have a different purpose than these proposed regulations. As a result, there is no redundancy in the two programs. Internationally, CBP requires aircraft operators to report cargo manifest data in advance of arrival into the United States under 19 CFR 4.7–7a. This requirement, however, may be fulfilled at the time the aircraft is already flying to the United States, when it may be too late to prevent an incident that would destroy the aircraft and potential ground-level targets. TSA and CBP are currently engaged in efforts to leverage their respective regulatory programs to further militate against an act of terrorism through air cargo. While CBP also has other security-focused regulations, the CBP mission and statutory authority concentrates on preventing the entry of high-risk goods from entering the United States upon arrival at the border. These CBP regulations do not govern the security requirements that air carriers must implement in order to prevent the introduction of explosives or operatives as cargo moves through the supply chain and onto aircraft for flight. TSA regulations and proposed amendments address this different security threat.

II. Efforts Leading to the Development of This NPRM

This NPRM is the result of more than a year of industry consultation, strategic planning and interagency coordination by TSA and DHS. The foundation of the policy changes recommended here are TSA's consultations with industry through its Aviation Security Advisory Committee (ASAC), the development of the DHS/TSA Air Cargo Strategic Plan, and coordination within the Department of Homeland Security.

A. The Aviation Security Advisory Committee

The Aviation Security Advisory Committee, a standing committee organized under the Federal Advisory Committee Act, was created in 1989, in the wake of the crash of Pan Am 103 over Lockerbie, Scotland, to provide the federal government with expert consultation on aviation security issues. Previously managed by the FAA, ASAC is now managed by TSA. ASAC is composed of 27 organizations with a stake in securing the aviation sector; members include groups representing victims and survivors of terrorist acts, freight forwarders, aircraft owners, airports, aircraft manufacturers, representatives of passenger and cargo airline management and labor, and representatives of key federal government agencies.

In April 2003, ASAC established three Air Cargo Security working groups: Shipper Acceptance Procedures (which focused on known shipper and other screening protocols), Indirect Air Carrier Security and Compliance, and Securing the All-Cargo Aircraft. ASAC working group members consisted of representatives from the following organizations and agencies, listed alphabetically: Air Courier Conference of America; Air Forwarders Association; Air France; Air Line Pilots Association; Air Transport Association; Airport Law Enforcement Action Network; Airports Council International—North America; Allied Pilots Association; American Association of Airport Executives; American Trucking Association; Association of Flight Attendants; Aviation Consumer Action Project; British Airways; Cargo Airline Association; Coalition of Airline Pilots Association; Federal Aviation Administration; Federal Bureau of Investigation; International Air Transport Association; Lufthansa; National Air Carrier Association; National Customs Brokers and Forwarders Association of America; National Industrial Transportation League; Regional Airline Association; Transportation Intermediaries Association; U.S. Customs and Border Protection; U.S. Department of Transportation—Office of the Secretary; U.S. Department of State; U.S. Postal Service; and Victims of Pan Am Flight 103.

On October 1, 2003, ASAC presented TSA with its final report on air cargo security, which included 42 recommendations covering 22 topical areas.[7] The working group's recommendations included strengthening the known shipper program by improving technology links between aircraft operators and the federal government, leveraging new technology to create a more layered cargo security approach, augmenting requirements to achieve known shipper status, strengthening the Indirect Air Carrier Standard Security Program (IACSSP) and securing the all-cargo aircraft operating area. The recommendations from the consensus report are reflected throughout this NPRM.

B. Air Cargo Security Strategic Plan

While the ASAC working groups were completing their independent assessments of air cargo security, TSA was developing an extensive strategic plan for securing air cargo (Air Cargo Strategic Plan). The Air Cargo Strategic Plan, which was completed in November 2003, and approved by the Department of Homeland Security in January 2004, evaluated TSA's and others' analyses of air cargo security, including the ASAC report. Based on these evaluations, the Air Cargo Strategic Plan details a threat-based, risk-managed program for securing the air cargo transportation system. The Air Cargo Strategic Plan contains a vision to ensure that TSA has adequately considered the security of air cargo operations. It identifies priority actions based on risk, cost, deadlines, performance, research and technology initiatives, and coordinated stakeholder outreach efforts. The Air Cargo Strategic Plan focuses on a multi-layered approach to security.

The Air Cargo Strategic Plan contains sensitive security information (SSI); therefore, its contents cannot be

[7] the ASAC report is protected at Sensitive Security Information under 49 CFR part 1520.

disclosed to the public.[8] In summary, it prescribes TSA's mission in the area of air cargo: providing the most effective security program possible while maintaining effective stewardship of resources and not unduly impeding the flow of commerce. The plan is multimodal, ensures that TSA has adequately considered the expanse of the air cargo security domain, and details a program for denying terrorists the opportunity to exploit that system. It identifies priority actions based on risk, cost, deadlines, performance, research and technology initiatives, and coordinated stakeholder outreach efforts in four strategic components: enhancing shipper and supply chain security, identifying elevated risk cargo through prescreening, identifying technology for performing targeted air cargo inspections, and securing all-cargo aircraft through appropriate facility security measures.

This NPRM proposes to implement many of the provisions of the Air Cargo Strategic Plan and ensures that the appropriate regulatory framework exists for additional measures that are not regulatory in nature. In addition to regulatory changes, aspects of the Air Cargo Strategic Plan will be implemented through security program updates, SDs and EAs, research and development programs, and public-private cooperative endeavors.

C. TSA–CBP Air Cargo Coordination

Since its establishment in November 2002 by the Homeland Security Act of 2002 (Pub. L. 107–296), the Department of Homeland Security has had, as one of its central tenets, the goals to reduce redundancy and improve effectiveness. This priority has particularly been the case in the area of air cargo security. Shortly after their transfer to the DHS, TSA and the U.S. Customs and Border Protection (formerly, the United States Customs Service) initiated an interagency program to leverage resources, eliminate unnecessary duplication and ensure compatibility between their respective air cargo security programs. The goal of this endeavor is to ensure that DHS has a comprehensive, coordinated policy for securing air cargo entering, transiting within and departing the United States. This NPRM complements CBP's programs, including the following primary coordination areas: the TSA known shipper program in conjunction with Customs-Trade Partnership Against Terrorism (C–TPAT); targeting, risk assessment, and compliance measurement; technology research and development; and explosives detection canine programs. This interagency coordination is instrumental to the implementation of TSA's layered approach to air cargo security and to many of the systems and processes that will support the regulatory changes proposed in this NPRM, and coincides with a Congressional mandate in the conference report accompanying the DHS appropriations act (H.R. Conf. Report No. 108–280 (2004) (''Air Cargo Report'')) that directed TSA to consider testing the expansion of C–TPAT to the domestic air cargo supply chain.

III. Summary of This Rulemaking

As explained further in section IV, this NPRM would enhance aviation cargo security significantly by requiring a number of measures. The NPRM would create a mandatory security program for all-cargo aircraft operations over 45,500 kg (100,309.3 pounds) and would amend existing security regulations and programs for other aircraft operators, foreign air carriers, airport operators, and IACs. The current rules for cargo carried on certain passenger aircraft, and for all-cargo operations under the existing Twelve-Five Standard Security Program[9] would be enhanced. Existing screening requirements for aircraft operators would be extended to cover all-cargo operations. Airports or aircraft operators would be required to secure the cargo operations areas. The definition of ''Indirect Air Carrier'' included in 49 CFR 1540.5 would be amended to include those transporting goods via all-cargo aircraft and all IACs would be subject to a more thorough vetting by TSA prior to receiving authorization to operate.

This NPRM also would require Security Threat Assessments for individuals who have unescorted access to cargo carried by certain aircraft operators, foreign air carriers, and IACs.

TSA is proposing these amendments after extensive consultation with industry through its Aviation Security Advisory Committee, and with other Federal agencies including the Department of Transportation and U.S. Customs and Border Protection. These amendments would significantly enhance aviation cargo security.

A. Who Is Affected by This NPRM?

TSA regulates four segments of the air cargo industry: (1) Airports serving cargo operations; (2) passenger aircraft operators that transport cargo; (3) all-cargo aircraft operators; and (4) IACs. Each segment is currently required to implement some type of TSA cargo security program. The current regulatory regime covers domestic entities in these four categories as well as foreign air carriers that operate into or out of the United States. The proposals in this NPRM would amend current security requirements for all of these industry segments, both through direct regulatory changes and through anticipated related security program changes.

B. Why Are These Regulatory Changes Necessary?

TSA has identified 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 in order to cause catastrophic damage. The magnitude of these risks is determined by factoring in the presence of credible threats and the existence of possible vulnerabilities that a terrorist could exploit. Many steps taken since September 11, 2001 have reduced the capabilities of international terrorist organizations; however, the terrorist threat remains. Likewise, new aviation security requirements have reduced the vulnerability of the air cargo system. Nonetheless, TSA, in cooperation with its many partners in the air cargo transportation industry, has identified additional enhancements of air cargo security to reduce further the likelihood of cargo tampering or unauthorized access to the aircraft with malicious intent. This NPRM addresses the remaining vulnerabilities in the air cargo system. TSA invites public comment on whether these concerns are appropriately addressed and adequately accounted for in this NPRM.

Terrorists have attempted to use air cargo to attack U.S. passenger aircraft on occasions in the past, and aviation generally continues to be a priority target for terrorists. The threat to air cargo represents a meaningful risk. TSA believes that strengthening air cargo security requirements through this proposed rulemaking will mitigate the threats.

C. How Did TSA Enhance Cargo Security After September 11, 2001?

Federal air cargo security requirements date back to the 1970's and have since evolved. Since

[8] SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would: constitute an unwarranted invasion of privacy; reveal trade secrets or privileged or confidential information obtained from any person; or be detrimental to transportation security. 49 CFR 1520.5(a)(1–3); 69 FR 28066, 28082–28083 (May 18, 2004).

[9] See discussions of Twelve-Five Standard Security Program at III.C. and IV.G.

September 11, 2001, the Federal Government has moved expeditiously to strengthen air cargo security even further. Immediately after September 11, FAA prohibited the shipment of all cargo aboard passenger aircraft. Later, this restriction was partially lifted to allow cargo from known shippers to be transported on passenger aircraft operators, but not cargo from unknown shippers.[10] By limiting air cargo aboard commercial passenger aircraft to known shippers only, FAA reduced the likelihood that cargo would pose a security threat to passenger aircraft. Since its creation, TSA has also taken several emergency measures to strengthen existing requirements, including additional qualifying requirements for the known shipper program.[11]

In the all-cargo aircraft environment, several all-cargo aircraft operators have voluntarily adopted the TSA Domestic Security Integration Program (DSIP)[12] to transfer cargo to passenger aircraft operators and to apply security identification display area (SIDA) requirements to all-cargo operations. The DSIP has been in place since 1992. FAA also strengthened the requirements for IACs immediately after September 11 by requiring additional steps to achieve IAC status. On February 22, 2002, TSA implemented the security program for Aircraft 12,500 Pounds or More, which became effective April 1, 2002 and applies to operators of aircraft with Maximum Certificated Take Off Weight (MTOW) more than 12,500 pounds in scheduled or charter service that are carrying passengers, cargo, or both and are not otherwise required to have a full or partial security program.[13] The rule also requires the pilot, flight engineer, or flight navigator assigned to duty during flight time on all regulated aircraft operators to have successfully completed a fingerprint-based criminal history records check (CHRC). It calls for restricted access to the flight deck if the aircraft has a flight deck door, and it mandates use of security coordinators, security training, procedures for bomb threats, and contingency plans.

In June 2002, TSA completed an extensive Air Cargo Security Scenario Analysis. The specific contents of this report are sensitive security information, and accordingly not publicly releasable. Where available, actual data were used for calculations; where data were not obtainable, estimates were identified and used. The analysis examined various scenarios, which focused on varying degrees of cargo screening, and which were selected to prevent or deter the introduction of explosive devices into the cargo holds of passenger aircraft. It was the first known attempt to conceptualize and conduct a detailed examination of the different security regimes, measure implementation costs and assumptions, and account for potential responses of the industry to the security changes, including the potential costs of implementation. The scenarios and variants ranged from screening unknown shipper cargo to screening cargo on passenger aircraft or preventing any cargo from being transported on passenger aircraft. The various scenarios were compared in terms of costs, benefits, and effectiveness.

TSA also has enhanced cargo security by implementing a web-enabled Known Shipper database to centralize data on persons and businesses that are authorized to ship air cargo on passenger aircraft to allow quick and efficient verification of a shipper's status while reducing redundancy. The initial version of the database was deployed in the Fall of 2002 and is currently being used by aircraft operators and IACs on a voluntary basis. Most of the major airlines, and 400 IACs, are participating. The database already consists of over 400,000 known shippers. In the near future, TSA plans to make use of the system mandatory for all aircraft operators, foreign air carriers and IACs required to participate in the known shipper program. This proposed rule would provide authority for this planned change, which would be implemented in the security programs of the aircraft operators, foreign air carriers and IACs.

At the core of this endeavor, the Known Shipper database will allow aircraft operators, foreign air carriers and IACs to submit electronically information on their known shippers to TSA and to verify electronically whether a client has been approved with known status under the program. This effort will offer a number of benefits, both for facilitating trade and improving security. Persons and businesses seeking Known Shipper status will no longer have to obtain this status from every aircraft operator, foreign air carrier or IAC with whom they do business; instead, once a shipper is accepted into the database, they will be considered known to all aircraft operators, foreign air carriers and IACs with access.

In November 2003, TSA required U.S. aircraft operators, foreign air carriers, and IACs to carry out certain additional security measures with respect to cargo. The U.S. intelligence community continued to receive and evaluate a high volume of reports indicating possible threats against U.S. interests. These reports, combined with recent terrorist attacks, created an atmosphere of concern. Terrorist groups such as Al Qaeda are capable of sophisticated tactics. The Department of Homeland Security was concerned about Al-Qaeda's continued interest in aviation, including using cargo aircraft to carry out attacks on critical infrastructure. In recognition of this threat, TSA made a determination that these circumstances required immediate action to ensure safety in air transportation. The additional measures TSA required in response to those concerns are described in IV. A.

D. What Would This Proposed Rulemaking Do To Strengthen the Current Air Cargo Security Regulatory Regime?

TSA is implementing a layered security solution throughout the life-cycle of the air cargo shipment and the aircraft on which it is being transported. As discussed in more detail in section IV. of this NPRM, TSA proposes to:

- Require security threat assessments for individuals with unescorted access to cargo;
- Codify cargo screening requirements first implemented under SDs, EAs, and part 1550 programs issued in November 2003;
- Require airports with SIDAs to extend them to cargo operating areas;
- Require aircraft operators to prevent unauthorized access to the operational area of the aircraft while loading and unloading cargo;
- Require aircraft operators under a full or all-cargo program to accept cargo only from an entity with a comparable security program or directly from the shipper;
- Codify and further strengthen the Known Shipper program;
- Establish a security program specific to aircraft operators in all-cargo operations with aircraft with a maximum certificated takeoff weight more than 45,500 kg;
- Strengthen foreign air carrier security requirements essentially to parallel the requirements on U.S. aircraft operators; and
- Enhance security requirements for Indirect Air Carriers.

[10] See Section IV. G.

[11] The specific criteria for the known shipper program are SSI under 49 CFR part 1520.

[12] The DSIP is a limited program under 49 CFR 1544.101(g). TSA has made this program available to all-cargo aircraft operators, in part, to allow those entities to interline cargo with passenger aircraft operations.

[13] 67 FR 8205 (Feb. 22, 2002).

TSA's proposed security requirements are infused throughout the supply chain instead of concentrating all efforts on one measure, such as physical inspection, at a single stage potentially resulting in significant disruption of the supply chain. This NPRM is a central component of this solution and proposes updating the requirements applicable to airports, aircraft operators, IACs, and foreign air carriers currently operating under a security program, and instituting new security requirements for all-cargo aircraft operators and the freight forwarders servicing them.

E. How Will TSA Enforce Compliance?

TSA relies on its staff of field inspectors to enforce compliance among regulated parties. As noted in various sections above, TSA also believes that issuance of a voluntary disclosure program, development and distribution of security training materials for certain IAC employees and agents, and implementation of enhanced electronic communication capabilities will materially enhance the regulated parties' compliance ability and orientation.

The ASAC working groups recommended that TSA implement a voluntary disclosure program to facilitate and improve compliance by regulated parties. TSA has received numerous similar requests from regulated parties. TSA agrees that aviation security is promoted by creating incentives for regulated entities to identify, disclose and correct their own instances of non-compliance, and to invest in efforts to preclude their recurrence. As a result, in December 2003, TSA implemented a voluntary disclosure program. Details of the program are available via the Internet on the TSA Web site at *http://www.tsa.gov,* with a link titled ''TSA Announces Civil Enforcement Policies'' in the section on Law & Policy. TSA's program is designed to encourage compliance with TSA regulations, foster secure practices, and encourage the development of internal evaluation programs. Upon detecting an inadvertent violation not yet known to TSA, a regulated entity must take immediate action to correct the violation. The regulated entity must report the violation to TSA in writing within 24 hours of detection and submit a detailed written report within 10 calendar days of the initial reporting. The regulated entity must develop a corrective action plan to ensure that the noncompliance remains corrected. After the regulated entity takes these steps, TSA may issue a letter of correction instead of a civil penalty action for the violation, provided all other elements of the policy are met. This program has been issued in a separate action and is not part of this rulemaking proposal.

F. Did TSA Consider Recommended Changes?

Yes, in addition to its own assessments, TSA based the policy changes proposed in this NPRM on recommendations received from the Department of Transportation Office of Inspector General (OIG), the General Accounting Office (GAO), and the Aviation Security Advisory Committee (ASAC). In addition, TSA has coordinated its efforts with other agencies in the Department of Homeland Security, including the U.S. Customs and Border Protection, which has statutory authority for screening cargo entering and departing the United States.

The Department of Transportation Office of Inspector General completed its audit of the air cargo security program in September 2002. This report is SSI. Accordingly, its distribution is restricted. In the report, the OIG offered 14 specific recommendations to increase the level of security as to ''insiders''—namely employees of aircraft operators and IACs with access to cargo. These recommendations varied from increasing the vetting of IACs seeking approval of their security program to training and testing requirements to improved compliance enforcement.

Further, in December 2002, the GAO issued its report, ''Vulnerabilities and Potential Improvements for the Air Cargo System (GAO–03–344).'' GAO traced the implementation of recommendations delivered during the 1990's and the development of technologies or operational procedures that might be used to enhance air cargo security. GAO did not make specific recommendations, but called for TSA to develop a comprehensive plan for air cargo security that includes priority actions identified on the basis of risk, costs, deadlines for completing those actions, and performance targets. TSA completed this strategic plan in November 2003. As noted previously, this document includes SSI and is not available to the public.

As previously discussed, TSA also considered the ASAC consensus report transmitted on October 1, 2003.

G. Were Other Solutions Considered and Why Were the Proposals in the NPRM Chosen Over Others?

TSA recognizes that the air cargo industry is large and complex, composed of numerous shippers, 226 domestic and foreign aircraft operators providing services through 2,789 stations at U.S. airports, and approximately 3,200 IACs with over 10,000 business locations. Together these entities transport approximately $30 billion worth of goods per year. In recognition of this breadth and complexity, TSA considered the full gamut of potential solutions for enhancing air cargo security in developing this NPRM. TSA analyzed the existing regulatory structure for air cargo security in the United States, partnered with industry, reviewed a variety of external assessments of the air cargo system, and coordinated with other agencies in the Department of Homeland Security with air cargo security experience and responsibilities, such as CBP, to develop solutions for today's challenges. TSA also reached out to numerous international entities including the European Commission, Transport Canada and International Air Transport Association to assess best practices and regulatory regimes that might be applicable to the U.S. environment.

The majority of participants in the ASAC air cargo security working groups have stated that proposals to require the inspection of every piece of cargo shipped on passenger aircraft are impractical. Instead, they recommended a risk-based targeting strategy to identify higher risk cargo for additional scrutiny; relying, in part, on the Government Accounting Office (GAO) report on Vulnerabilities and Potential Improvements for the Air Cargo System,[14] the Department of Transportation's Office of the Inspector General (OIG) Audit of the Cargo Security Program,[15] and TSA's Air Cargo Security Scenario Analysis. These reports have cautioned that, in the absence of an appropriate targeting methodology and data, a requirement for inspection of 100% 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, and could have particularly severe negative impacts on aircraft operators, IACs and their employees and agents. TSA agrees with this assessment. TSA believes that a requirement to inspect every piece of cargo could result in an unworkable cost of more than $650 million in the first year of implementation.[16]

[14] GAO–03–344 December 2002.

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

[16] See Regulatory Evaluation for the Air Cargo Security Requirements NPRM, Table 1, Ten-Year Undiscounted Cost Summary for passenger and all-cargo flight cargo screening.

In its final presentation to TSA, ASAC noted that the layered solution outlined in its forty recommendations would significantly enhance air cargo security while ensuring that commerce is not disrupted, two goals TSA is committed to achieving. It was the sense of the ASAC that technology solutions must be pursued as aggressively as possible. Specifically, the committee's recommendations included using technology to improve communication links between regulated parties and the federal government, leveraging new technology to create a more layered cargo security approach, and using technology to enable enhanced requirements for achieving Known Shipper status.

Similarly, TSA reviewed FAA's October 2001 ''Air Cargo Threat Assessment'' (DOT/FAA/AR–02/15) analysis of the vulnerabilities of the current air cargo security program.[17] In this report, FAA's overall assessment was that an integrated security regime was required. These FAA recommendations have been considered and are reflected in portions of this NPRM.[18]

The Department of Transportation Office of the Inspector General audited the FAA's air cargo security program. The OIG's report of this audit and its results, including data sources, are SSI. Like the ASAC and FAA, the OIG determined that air cargo security could best be bolstered by implementing layered solutions throughout the air cargo system; and offered fourteen specific recommendations. TSA concurred with the OIG's assessment and these recommendations are reflected in both TSA's air cargo strategic plan and in this NPRM.

TSA will continue to use SDs and EAs as required to address immediate threats. These directives are issued to regulated parties outlining specific requirements that must be met as part of their security programs and are protected as sensitive security information.

Like TSA, CBP also relies on a layered security program for securing air cargo and both agencies are committed to determining how best to leverage individual resources and avoid unnecessary redundancy. As a result, TSA and CBP have initiated a dialogue for coordinating their respective air cargo security activities. TSA and CBP initiated this effort shortly after DHS was established and the agencies received a Congressional mandate to continue this effort during Fiscal Year 2004. TSA and CBP are looking closely at how best to apply their combined experience in promoting supply chain security, securing cargo prior to loading, and applying risk-based targeting programs. In addition, through this effort, DHS is committed to ensuring the maximum degree of consistency between TSA and CBP programs and minimizing the impact on industry by coordinating requirements and procedures.

Within the BTS Directorate, CBP and TSA have distinct, but equally vital, security missions in securing air cargo. Historically, CBP has primarily been responsible for determining the admissibility of the cargo held on the aircraft and as such is concerned about cargo that may carry threats to be deployed once the cargo reaches U.S. borders. TSA, on the other hand, is responsible for securing both domestic 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 or stowaways on board.

The priority mission of CBP is to prevent terrorists and terrorist weapons from entering the United States. That mission means improving security at the nation's physical borders and ports of entry, but it also means extending the zone of security beyond our physical borders—so that American borders are not the first line of defense. With regard to the securing of international air cargo, CBP has a long history of screening and inspecting cargo upon arrival in the United States. Today it continues this challenge with a refined focus on stopping terrorists and terrorist weapons at our nation's borders.

TSA's mission is to provide security in all modes of transportation, with a priority emphasis on aviation. Like CBP, TSA employs a threat-based, risk-managed approach to securing air cargo. Therefore, we focus our efforts in the passenger environment on preventing the introduction of explosive devices into the cargo bays of passenger air carriers. In the all-cargo environment, while measures are taken to prevent the introduction of an explosive device on an all-cargo aircraft, our primary concern is focused on keeping intruders or stowaways off the aircraft, as a hijacking causes significant loss of life and other damage on the ground and in the air.

Extensive interagency analysis and outreach to both industry and other federal agencies have led TSA to conclude that a threat based, risk managed, layered solution will provide the highest degree of security in the air cargo environment while causing the least financial and procedural impact on a business sector that contributes significantly to the United States and global economies. TSA invites public comment on the feasibility of this approach overall, on the specific rule changes and requirements proposed in this NPRM, and on other possible actions, such as a requirement to inspect 100% of air cargo, that have been the subject of public discussion but which TSA, for reasons outlined above, has determined not to propose in this NPRM.

IV. Summary of Proposed Amendments

A. Current Regulation of Aircraft Operators and Foreign Air Carriers and Proposed Amendments

TSA regulations currently cover a variety of aircraft operators as part of an overall, layered approach to security. Aircraft operators with scheduled or public charter passenger operations using aircraft with a passenger seating configuration of 61 or more, or those using smaller aircraft that enplane passengers from or deplane passengers into a sterile area, must have *full programs* under § 1544.101(a). These operators often carry cargo in addition to passengers and must comply with cargo security requirements under § 1544.205.

Aircraft operators using aircraft in scheduled or public charter passenger operations using aircraft with a passenger seating configuration of 31 or more but 60 or fewer seats must have a *partial program* under § 1544.101(b).

Aircraft operators using aircraft with a maximum certificated takeoff weight of 12,500 pounds or more, in scheduled or charter service, carrying passengers or cargo or both, must have a *twelve-five program* under § 1544.101(d) & (e).

Aircraft operators using aircraft in private charter passenger operations using aircraft with a passenger seating configuration of 61 or more or a maximum certificated takeoff weight greater than 45,500 kg (100,309.3 pounds) must have a *private charter program* under § 1544.101(f), as well as having a twelve-five program.

This NPRM is proposing to add another type of program. As discussed further in this preamble, TSA is proposing that aircraft operators operating all-cargo aircraft with a maximum certificated takeoff weight of more than 45,500 kg (100,309.3 pounds) have an *all-cargo program* under proposed § 1544.101(h) & (i).

Certain foreign air carriers must have security programs as well. Those with

[17] This document is SSI and, accordingly, not publicly releasable.

[18] This report is protected as Sensitive Security Information under 49 CFR part 1520.

scheduled or public charter passenger operations using aircraft with a passenger seating configuration of 61 or more, or those using smaller aircraft that enplane passengers from or deplane passengers into a sterile area (analogous to U.S. operators with full programs), must have security programs under § 1546.101(a) or (b). Those in scheduled or public charter passenger operations using aircraft with a passenger seating configuration of 31 or more but 60 or fewer seats must have programs under § 1546.101(d) (analogous to U.S. operators with partial programs).

In addition, in November 2003, in response to threats, TSA required foreign air carriers that perform all-cargo operations using aircraft with a maximum certificated takeoff weight of 12,500 pounds or more to carry out the All-Cargo International Security Procedures issued by TSA. 69 FR 3939 (Jan. 27, 2004). In this NPRM, TSA is proposing to codify this procedure and to create foreign air carrier security programs analogous to a U.S. twelve-five program in all-cargo operations and to the proposed all-cargo program in part 1544.

Additionally, in November 2003, TSA issued SDs and EAs requiring domestic aircraft operators under a full program or a twelve-five all-cargo program and foreign air carriers to apply further screening measures to cargo. More specifically, TSA required that these operators inspect a percentage of cargo prior to loading it on an aircraft.

Aircraft operators under a full program must also continue to abide by the requirements of the Known Shipper program. Generally, these aircraft operators may transport only cargo from a known shipper. Congress specified in ATSA, codified at 49 U.S.C. 44901(a), that a Federal employee is not required to carry out screening requirements for a passenger aircraft operator of the Known Shipper program. These screening functions may be performed by the private sector. Likewise at 44901(a), Congress distinguished that Federal screeners must conduct certain passenger screening. Operators of all-cargo aircraft do not share this distinction. All-cargo aircraft operators also may perform cargo screening; it is not required that a Federal employee carry out screening of all-cargo aircraft.

The security procedures required for the varying programs are focused to address the greatest perceived threats to the respective operations. Accordingly, TSA requires the most security procedures under the layered approach to those operations perceived to have the highest threat. For instance, the full program focuses security requirements both to protect the large number of passengers on board the aircraft as well as to prevent the largest of aircraft from being hijacked and used as a missile to attack another target, and thus are subject to the most intense security measures. The proposed *all-cargo program* would focus on the latter threat because aircraft operators under this proposed program generally use the same types of aircraft as those used under a full program. All-cargo operations under the twelve-five program require layers of security appropriate to the lower threats posed by smaller aircraft. TSA has developed a measured approach to match security requirements with the possible risks.

B. Security Threat Assessments for Air Cargo Workers

TSA currently requires a variety of individuals working in aviation to submit to a criminal history records check. Generally, these individuals work on airport grounds and have access to secure areas.

In the cargo environment, many other persons have access to cargo before someone who works for the airport and has had such a check handles it. In this rulemaking, TSA proposes to require additional persons who have unescorted access to air cargo, but do not have unescorted Security Identification Display Area (SIDA) access, to undergo a security check to verify that they do not pose a security threat.

TSA recognizes that the number of individuals with access to cargo is large—approximately 63,000—and that the companies that they work for run the gamut from complex organizations to ''mom and pop's.'' Therefore, requiring all these individuals to undergo fingerprint-based criminal history background checks would be a time-consuming and costly process. TSA believes that potential security concerns related to unescorted access to cargo by these individuals would be best addressed at this time by requiring the individuals to submit to a Security Threat Assessment program, focused on the threat of terrorism. A Security Threat Assessment, as proposed in this NPRM, would rely on checks of existing intelligence-based records and databases to ensure that an individual who is a known or suspected threat is prohibited from working in positions that could allow that individual to have unescorted access to air cargo. This program adopts best practices from the financial services and transportation security communities to reduce the likelihood that a terrorist could gain access to cargo.

In proposed §§ 1544.228, 1546.213, and 1548.15, TSA would prohibit aircraft operators under a full program or all-cargo program; foreign air carriers operating under §§ 1546.101(a) (b) or (e); and each IAC from authorizing any individual to have unescorted access to cargo unless the respective operator has verified the identity of that individual in a manner acceptable to TSA, and that individual has successfully completed a CHRC under 49 CFR 1542, 1544, or 1546, Security Threat Assessment pursuant to proposed Subpart C of part 1540, or another Security Threat Assessment approved by TSA.

TSA has also considered extending security threat assessment requirements in additional contexts. For instance, TSA considered requiring every employee of an entity regulated by TSA that is in the business of cargo transportation to submit to a security threat assessment. TSA proposes that the layered approach of requiring assessments for those individuals with unescorted access to cargo, combined with requirements to secure cargo upon acceptance, are at this time sufficiently focused on the potential security threat.

TSA also considered requiring each person who boards for transportation on an aircraft under an all-cargo security program to submit to a security threat assessment. Alternatively, TSA considered 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. TSA has not proposed these measures but invites comments on these considerations.

C. Security Measures for Persons Boarding an All-Cargo Aircraft

TSA is proposing to codify requirements for screening persons other than passengers boarding the all-cargo aircraft with a maximum certificated take-off weight greater than 12,500 pounds. See proposed § 1544.202 and § 1546.202. Under FAA rules, some persons who are not flight crew members or passengers may travel on an all-cargo aircraft, such as handlers escorting an animal being shipped via air cargo. See 14 CFR 121.583 and 121.587. Such individuals could be in a position to attempt to take over the aircraft. TSA believes that it is necessary to screen such persons to ensure that individuals traveling on aircraft under an *all-cargo program,* or under a *twelve-five program* in an all-cargo operation, do not present a security threat. Such screening is now being done under SDs issued in November 2003 and is included as a proposed regulatory requirement in this NPRM. While

Congress specified in 49 U.S.C. 44901(a) that a Federal employee must conduct screening of persons in passenger operations, section 44901(f) has no such requirement for all-cargo operations. Accordingly, the private sector may conduct screening in all-cargo operations in compliance with TSA standards.

D. Screening Cargo

To guard against unauthorized weapons, explosives, persons, and other destructive substances or items in cargo, TSA proposes to codify a requirement for aircraft operators to inspect a portion of air cargo, including that offered by known shippers. See proposed §§ 1544.205 and 1546.205. An SD issued to operators with full programs in November 2003 requires that a portion of known shipper cargo be inspected, and this NPRM would codify that change. In addition, an SD issued requires operators of Twelve-Five all-cargo aircraft inspect a portion of cargo. When conducting inspections, aircraft operators are required to follow TSA-approved requirements.

In addition, aircraft operators operating under full programs are currently required to submit individuals conducting cargo screening to a fingerprint-based CHRC under § 1544.229 to reduce the likelihood that a terrorist could gain such employment to facilitate the introduction of unauthorized persons, explosives, incendiaries, and other substances or items. This proposed rule would also require aircraft operators operating under all-cargo programs to submit their cargo screeners to a CHRC under § 1544.229, mitigating the possibility that an authorized person would threaten or otherwise compromise the security of the aircraft operations.

TSA considered several other requirements for cargo screening that are not included in this NPRM. For instance, TSA considered prohibiting all cargo from transportation on passenger aircraft. TSA recognizes, however, that this requirement would likely lead to significant economic impact on passenger operations. Moreover, TSA proposes that a layered approach to security requirements, including those proposed in this NPRM, would provide for an appropriate level of security and could be implemented without undue hardship on the affected stakeholders. TSA also considered requiring physical inspection of 100% of all cargo on all aircraft, or alternatively on passenger aircraft. However, as noted in III.G. above, 100% inspection of cargo would be impractical and would severely impact the rapid delivery of air cargo. TSA invites comment on these considerations.

E. Securing the Cargo Operating Environment

Measures to prevent unauthorized individuals from gaining 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. Currently, at airports that have complete programs under 49 CFR 1542, and therefore are required to have a SIDA based on the presence of covered passenger operations, all individuals working in the SIDA must have an airport-approved photo identification (ID) media that meets standards established by TSA. This ID must be displayed at all times above the waist on the individual's outermost garments. To obtain a SIDA ID, a person must successfully undergo a fingerprint-based CHRC and successfully complete training in accordance with the airport's security program (*see* 49 CFR 1542.205, 1542.211, and 1542.213). In addition, procedures must be in place for challenging all persons not displaying appropriate ID for the area in which they are found. Currently, all-cargo operations are not specifically covered under airport SIDA requirements.

At airports that are required to have a SIDA because of the presence of covered passenger operations, TSA proposes in this NPRM to extend SIDA requirements to cargo operating areas. See proposed § 1542.205. As previously discussed, the potential consequences of an all-cargo aircraft being hijacked and used as a missile to attack another target are comparable to the consequences of a hijacking of a passenger aircraft of the same size. Accordingly, TSA proposes to add a layer of security to protect these aircraft further by applying SIDA requirements in cargo operating areas. Airports that currently have SIDA have the associated procedures and requirements in place. TSA believes that airports that have SIDA will be able to extend SIDAs to areas where cargo is loaded and unloaded without great challenges. Indeed, the cargo operation areas at many of these airports already are SIDAs. TSA also considered extending SIDA requirements to airports that serve all-cargo carriers and are not currently required to have a SIDA. Airports without SIDAs, however, would be required to implement many unfamiliar requirements in order to create SIDA. These airports also may have only occasional and unpredictable all-cargo aircraft traffic, such as on-demand charter operations. In this NPRM, TSA proposes that aircraft operators implement other measures that will enhance security instead of requiring airports without SIDAs to create them. Accordingly, TSA proposes in § 1544.225 to require that the aircraft operator prevent unauthorized access to the operational area of the aircraft while loading or unloading cargo. Note that aircraft operators now must comply with § 1544.217, which requires covered aircraft operators to arrange for a law enforcement presence to respond to any situations that may arise. TSA believes that the aircraft operator is well positioned to provide sufficient security for their aircraft operations, in lieu of an airport SIDA. TSA invites public comment on the economic, operational, and security implications of this approach. TSA also proposes to require that, before placing an all-cargo aircraft back into service after a period spent unattended, the aircraft operator conduct a security inspection of the aircraft. See proposed § 1544.225 and § 1546.103(a)(1). Together, these provisions would reduce the likelihood of successful tampering, stowaway boarding, or the introduction of an improvised explosive device or other destructive substance or item. Similar provisions are currently required of passenger aircraft operators operating aircraft of the same size.

F. Accepting Cargo From Comparable Entities

TSA is proposing to authorize aircraft operators under full or all-cargo programs to accept cargo only from the shipper, or from an entity with a security program comparable to the aircraft operator's. See proposed § 1544.205(e) and § 1546.205(e). The purpose of this proposed amendment is to prohibit aircraft operators from carrying cargo transferred from persons or businesses without the appropriate security measures to guard against the introduction of unauthorized weapons, explosives, persons, or other destructive substances or items. TSA will provide these aircraft operators in their security programs with a more detailed account of what cargo may be accepted.

G. Known Shipper Program

TSA proposes to codify and strengthen the Known Shipper program in regulation at 49 CFR 1544.239, 1546.215, and 1548.17. As discussed above in section III., paragraph C., ''How did TSA enhance cargo security after September 11, 2001?,'' the Known Shipper program is a protocol to distinguish shippers about whom security-relevant information is known from those shippers about whom the aircraft operator has inadequate

information. This program applies to aircraft operators with full programs, corresponding foreign air carriers, and IACs that offer cargo to such aircraft operators and foreign air carriers.

TSA considered extending a regulatory program directly to shippers of cargo that intend to use air transportation. By doing so, TSA would have direct oversight and regulatory authority throughout the cargo supply chain. The number of potential shippers, however, may be unwieldy. Potentially any person or business may ship cargo by air. TSA proposes, instead, to focus on aircraft operators and IACs as discussed through this NPRM.

Certain operational elements of the Known Shipper program are sensitive security information and cannot be divulged. However, the existence of the program is a matter of public record. Congress recognized the existence of the Known Shipper program in the Aviation and Transportation Security Act, Pub. L. 107–71, at section 110. Since September 11, 2001, cargo from unknown shippers has not been permitted to be transported aboard aircraft operated under a full program.

TSA considered allowing unknown shipper cargo on passenger aircraft after physical inspection. TSA recognizes that this cargo could provide considerable business opportunity to aircraft operators, but determined that this measure could not assure adequate security. No single technology currently exists with sufficient versatility to handle the vast array of cargo sizes, shapes, and materials to ensure security while maintaining acceptable throughput, or processing time. TSA welcomes comments and recommendations on this issue.

Although the Known Shipper program has been in existence for over 10 years in its current form and has its roots in security programs that date back to 1976, it has not previously been identified in security regulations; rather, it has been in the aircraft operator security programs. TSA is proposing to codify and enhance the Known Shipper program in this NPRM.

TSA will consider, but TSA is not proposing to allow cargo submitted by unknown shippers to be transported on passenger aircraft under a full program at this time. TSA invites public comment on the costs, benefits and practical implications associated with screening cargo from unknown shippers to the degree necessary to permit it to be transported on commercial passenger aircraft.

As discussed in III.C. above, TSA is implementing a comprehensive strengthening of the Known Shipper program. These improvements centralize and automate the vetting of applicants to the Known Shipper program. Under this NPRM, when proposing a shipper for the Known Shipper program, an aircraft operator, foreign air carrier, or IAC would be required to submit an application electronically to TSA for vetting against terrorist and law enforcement data. This information will then be stored in a central database along with the shipper's status in the program. Aircraft operators, foreign air carriers, and IACs would be required to check a shipper's status on the system before accepting its cargo for transport on passenger aircraft. This proposed requirement will enable TSA to conduct a thorough threat assessment of those seeking to ship by passenger aircraft.

To assist in implementing the enhancements to the Known Shipper program, TSA proposes in this NPRM that, when TSA so requires, the aircraft operators, foreign air carriers, and IACs will submit known shipper information electronically and update it as needed. TSA has designed its known shipper database, including the necessary Internet elements, to ensure that shipper lists are not compromised. TSA believes that the proposed changes would facilitate industry participation in the Known Shipper program by reducing the administrative burden on individual aircraft operators.

H. Establish All-Cargo Operator Standard Security Program

Aircraft operators using passenger aircraft with a passenger seating configuration of sixty-one seats or more in scheduled or public charter service must have a full program under 49 CFR 1544.101(a), using the Aircraft Operator Standard Security Program (AOSSP). Aircraft operators using passenger aircraft that have a maximum certificated takeoff weight greater than 45,500 kg (100,309.3 pounds), or a passenger-seating configuration of 61 or more, that are not government charters or in private charter service, must have a program under 49 CFR 1544.101(f). Currently, however, all-cargo aircraft operators operating aircraft of a similar size and potential destructive power are subject to the Twelve-Five program, rather than the full program. These operators are currently required to implement security programs in accordance with TSA's Twelve-Five Standard Security Program governing aircraft with a maximum take off weight of 12,500 pounds or more. In addition, some cargo operators voluntarily participate in the more comprehensive DSIP. Considering the potential risks associated with heavier all-cargo aircraft, TSA proposes to require additional steps for securing all-cargo aircraft weighing more than 45,500 kg (100,309.3 pounds) at § 1544.101(h). These measures would be incorporated into a mandatory All-Cargo Aircraft Operator Standard Security Program. The program will include elements of the DSIP.

Extending pertinent requirements to all-cargo aircraft operators operating above the 45,500 kg threshold would institute security measures for all-cargo aircraft comparable to passenger aircraft of the same size. An all-cargo aircraft with maximum certificated takeoff weight greater than 45,500 kg could cause significant damage if taken over and used as a weapon. TSA also applies this applicability threshold in the private charter program,[19] 49 CFR 1544.101(f), and it is consistent with international security standards adopted by the International Civil Aviation Organization.[20]

TSA recognizes that the operations of all-cargo aircraft operators and passenger aircraft operators are not identical and looks forward to working with industry to ensure that proposed new requirements are tailored to accommodate those differences.

I. Strengthen Foreign Aircraft Operator Security Measures

TSA currently requires foreign air carriers using aircraft of a certain size and engaged in scheduled or public charter passenger operations and landing or taking off in the United States to have a TSA-approved security program. Foreign all-cargo air carriers are subject to certain security requirements identified in a security program issued by TSA under part 1550 in November 2003, including random inspection of cargo. *See* 69 FR 3939 (Jan. 27, 2004). TSA is proposing to amend § 1546.101 to make these requirements permanent and incorporate them into the foreign air carrier regulations in recognition that these measures were implemented on an emergency basis and should now be available for public comment as part of this rulemaking.

TSA proposes to extend to foreign all-cargo air carriers requirements to implement a level of security similar to that of U.S. aircraft operators using the same size aircraft. Under the proposed amendment to § 1546.101, foreign air carriers would be required to adopt and implement a security program acceptable to TSA for all flights using an

[19] 67 FR 41635, 41637 (June 19, 2002).

[20] 67 FR 79881, 79883 (December 31, 2002).

all-cargo aircraft with a maximum certificated takeoff weight of more than 45,500 kg that land or take off in the United States. This security program would essentially parallel the requirements of the proposed all-cargo program for U.S. aircraft operators. This NPRM also proposes that foreign air carriers in all-cargo operations with aircraft over 12,500 pounds and up to 45,500 kg also implement security programs. This security program would essentially parallel the requirements of the Twelve-Five Standard Security Program for U.S. aircraft operators. The remaining proposed amendments would require foreign air carrier security programs to provide a level of security similar to that required of U.S. aircraft operators serving the same airport and employ equivalent procedures. These procedures include application of security measures to persons and property on board the airplane under proposed § 1546.202, measures for acceptance and screening of cargo under proposed § 1546.205, introduction of security threat assessments for cargo personnel in the United States under proposed § 1546.213, and application of Known Shipper program requirements under proposed § 1546.215.

J. Enhancing Existing Requirements for IACs

The IAC, sometimes called a freight forwarder, is a crucial part of the air cargo system, acting as an intermediary between the shipper and the aircraft operator for approximately 80% of all air cargo shipped on passenger aircraft in the United States. TSA estimates that there are 3,200 entities in the United States operating as IACs ranging from large corporations to sole proprietors working out of their homes. All IACs are required to maintain a security program known as the IACSSP and are regulated under 49 CFR 1548. This NPRM proposes to expand the definition of IAC to include businesses engaged in the indirect transport of cargo on larger commercial aircraft, regardless of whether the operation is conducted with a passenger aircraft or an all-cargo aircraft.

In addition, TSA plans to strengthen security requirements for all IACs. Specifically, TSA proposes to vet businesses more thoroughly before they are authorized to do business as IACs, strengthen a requirement for periodic recertification of IAC status, and strengthen security requirements for accepting and processing air cargo. These amendments to the rules governing IAC operations are intended to improve the security of the air cargo supply chain by infusing better security during the period between when a package leaves a shipper and when it is presented to the aircraft operator.

A key element of TSA's proposed enhanced IAC standard security program is a more thorough vetting of entities seeking authority to do business as IACs. To strengthen the application process, TSA is developing a web-based, centralized system for validating and revalidating IACs. This system will improve security through an enhanced, more effective vetting process while facilitating the application, renewal and review process for the industry.

Upon implementation of the Internet-based system, TSA proposes, under § 1548.7, to require all businesses to use the system to obtain initial IAC approval and to renew their approval. In doing so, TSA proposes to require IAC applicants to submit more information about themselves and their business than is currently required, including basic corporate records. IACs would also be required to use the system to notify TSA of any changes to their corporate structure and to renew their status annually. These two steps will allow TSA to check whether the applicant is a legitimate business and determine whether the business or personnel poses a threat to transportation security.

These planned new IAC vetting tools, combined with the centralization of information and automated communications, would enable TSA to implement effectively a program to remove IAC authorization from those persons found to be security risks during revalidation or found to be out of compliance. In this NPRM, TSA proposes procedures for withdrawing IAC security program approval.

TSA's envisioned electronic validation/revalidation process is also indicative of the DHS commitment to improving security while promoting best business practices. By automating much of the current paper-based process, TSA would be able to accelerate the validation and revalidation process, and industry would have an improved means of communication with TSA that facilitates TSA's ability to notify IACs and aircraft operators of pending actions.

K. Establishing New Training and Personnel Requirements

TSA is proposing to add regulatory text to: expand general security requirements to include the protection of stored or en route cargo under § 1548.9; implement training under § 1548.11; require IACs to appoint Security Coordinators under § 1548.13; authorize IACs to receive and require IACs to confirm receipt of, and to implement SDs and Information Circulars under § 1548.15.

To ensure that IAC employees understand and are trained to implement their security responsibilities, TSA is proposing to require a comprehensive and recurrent training program for IACs. This program would cover procedures for accepting, accessing and handling cargo intended for transport on aircraft as well as record keeping, acceptance and maintenance of Sensitive Security Information, and communication protocols and other requirements in the security program. As part of this initiative, TSA proposes to develop computer and/or video-based instructional materials and a testing tool, including a minimum standard that an employee will be expected to meet, and protocols for situations where employees fail to meet the threshold. Development of these training tools will coincide with the review and consideration of this NPRM and revisions to the IACSSP; training materials should be available to IACs shortly after these changes are implemented. TSA believes that development and distribution of these training tools will enhance regulatory compliance among the IAC community. TSA invites public comment on the practical and economic implications of requiring training of IAC and IAC agent personnel, and on the best means for achieving a high training standard without disrupting commerce.

TSA also proposes to require IACs to designate a Security Coordinator at the corporate level. This individual will be responsible for implementing the IAC's security program and will serve as the IAC's primary point of contact for communication with TSA. The Security Coordinator can be an existing employee with additional duties, but someone in this role must be available 24 hours a day. Establishment of IAC security coordinators is crucial to ensuring that TSA has an open line of communication with this important class of regulated parties. Currently, airport operators and aircraft operators must have Security Coordinators.

As TSA is presented with new threat and vulnerability information, TSA may need to require IACs to adjust their actions accordingly. Currently, TSA communicates such information to regulated parties, particularly to aircraft operators, by issuing SDs and Information Circulars. TSA is proposing to implement a parallel capability for IACs. IACs would be authorized to receive SDs, and required to verify receipt of the directive or circular and

to notify TSA how they will comply with it. If an IAC is unable to comply with a SD, it would be allowed to propose an alternative means of compliance to TSA. Formalizing this two-way communication is necessary to ensure sufficient measures are enacted when the threat changes, such as during a heightened state of alert.

TSA also proposes to codify existing general requirements of the IACSSP to require IACs to enhance the security of cargo stored or en route to the aircraft operator. The proposal to enhance en route and storage security is intended to ensure that IACs are held accountable for securing the goods entrusted to them throughout those legs of the supply chain for which they are responsible. Acceptable security measures are likely to include standards for facility security, and lock and seal requirements for conveyances. TSA invites suggestions from interested parties regarding the most appropriate solutions available.

V. Section-by-Section Analysis of Proposed Changes

Part 1540—Civil Aviation Security: General Rules

Section 1540.5—Terms Used in This Subchapter

TSA proposes to broaden the definition of ''Indirect Air Carrier'' by removing the word ''passenger,'' in order to expand TSA security program requirements to freight forwarders that offer cargo to all-cargo aircraft operations. The ASAC Air Cargo Security working groups (''ASAC working groups'') recommended, and TSA agrees, that limiting the definition of IAC to only those persons that tender cargo to a passenger aircraft would be inconsistent with TSA's goal of extending a security regime to all-cargo aircraft operations.

Sections 1540.201 Through 1540.209—Subpart C—Security Threat Assessments

The ASAC working groups recommended, and TSA agrees, that the identities of personnel who have unescorted access to cargo to be shipped by air should be verified, and that such personnel should be subject to appropriate background checks. TSA proposes to create a type of personnel background check to be called a ''Security Threat Assessment.'' This Security Threat Assessment would include a search by TSA of domestic and international databases to determine the existence of indicators of potential terrorist threats that meet the standards set forth in proposed Subpart C of part 1540. This subpart is procedural and sets out the scope and basic procedural requirements of a Security Threat Assessment, including related fee requirements, and provides for review of TSA determinations in connection with Security Threat Assessments.

In proposed §§ 1544.228, 1546.312, and 1548.15, operators would be required to ensure that individuals who have unescorted access to cargo undergo a Security Threat Assessment or other check. See the discussion of § 1544.228 below. This requirement would apply to aircraft operators operating under full or all-cargo programs, the corresponding foreign air carriers, and IACs that offer cargo to such operators.

TSA's proposed Security Threat Assessment would require in § 1540.203 that operators verify the individual's identity, after which TSA would check their identity information against intelligence records and other data related to terrorism. Operators would be required to submit the individual's name, date and place of birth, social security number and date of naturalization (if a naturalized citizen), citizenship status, alien registration number (if applicable) and a detailed description of the measures taken to verify the individual's identity. After assessing this data to determine whether the individual poses or is suspected of posing a threat to national security, transportation security or of terrorism, under proposed § 1540.205, TSA would notify the regulated party and the individual. This notification can take 3 forms:

1. *Security Authorization for Unescorted Cargo.* This notification would indicate 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 Denial of Authorization for Unescorted Cargo Access.* This notification would be issued if TSA knew or suspected the individual of posing a threat. The individual would be able to appeal this determination through adjudication, but the individual would not be permitted unescorted access to air cargo while the appeal is pending.

3. *Final Denial of Authorization for Unescorted Cargo Access.* 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 notification would inform the operator and the individual that he or she must be barred from having unescorted access to air cargo.

Section 1540.207 would set out the appeals procedures under this proposal to provide appropriate due process. Section 1540.209 would establish the fee requirements necessary to recover associated costs of the Security Threat Assessment. Under the proposed rule, the operator would not permit the individual to handle cargo until the operator and the individual were notified of a Security Authorization for Unescorted Cargo Access by TSA. In cases where TSA issues a Denial of Authorization for Unescorted Cargo Access, TSA may notify government agencies for law enforcement or security purposes, or in the interests of national security. TSA recognizes that the requirement for background checks 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

Currently, part 1542 applies to airport operators regularly serving aircraft operators with full programs, private charter programs, or partial programs under part 1544, or the corresponding foreign air carriers under part 1546. Airport operators under part 1542 must have and carry out security programs as described in that part and, under § 1542.5, must allow TSA to conduct inspections on the airport. Airports that do not regularly serve such operations, or only serve twelve-five programs, are not now subject to part 1542.

TSA proposes to revise § 1542.1 by adding subparagraph (d) to require that each airport that serves an aircraft operator with any security program under part 1544 or a foreign air carrier under part 1546 would be subject to § 1542.5. This would ensure that TSA could inspect aircraft operators and foreign air carriers using an airport that does not have a security program. It is critical that TSA have access to those aircraft operations to determine whether they are in compliance with the security requirements. Accordingly, the proposed addition of subparagraph (d) would provide that TSA may enter an airport that is not otherwise subject to part 1542 to conduct an inspection on an aircraft operator or a foreign air carrier regulated under parts 1544 and 1546, respectively. This proposal would not require that any additional airport operators obtain security programs; it

would only require that certain airport operators allow TSA to conduct inspections under § 1542.5.

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

The ASAC working groups recommended, and TSA agrees, that, at airports that currently have one or more SIDAs, the SIDA should be extended or a new SIDA created to encompass air cargo operations. These airports have complete programs under § 1542.101(a) and serve the passenger aircraft operators with full programs. Under current § 1542.205, for each SIDA the airport operator must establish and carry out a personnel identification system, subject each individual who has unescorted access to a criminal history records check, and ensure each individual with unescorted access is properly trained. Currently, air cargo operations are not required to be conducted in SIDAs.

Under paragraph 1542.205(a) TSA is proposing to add a new paragraph (a)(2) that expands the scope of operations that must be in a SIDA by requiring airports with SIDAs either to expand existing or create new SIDA to incorporate areas of cargo operations. These cargo operations areas would include areas where cargo is regularly sorted, loaded, or unloaded by certain aircraft operators or foreign air carriers. The SIDA would only be extended to areas on airport grounds.

This proposed change would apply only to aircraft operations conducted under a full program, and those operating under an all-cargo program. Also, only areas of the airport that are regularly used for these cargo operations would be made SIDAs. Areas on these airports that are only occasionally used would not need to be SIDAs, but the aircraft operator would be required to provide security for the area under proposed § 1544.225(d). Similarly, at airports that do not have SIDAs pursuant to §§ 1542.103(a) and 1542.205(a), aircraft operators would provide security under proposed § 1544.225(d). All airport operators who would be affected by the proposed amendment of paragraph 1542.205(a) currently have a SIDA and are already subject to the requirements of § 1542.103(a) and § 1542.205.

TSA also proposes to revise current paragraph 1542.205(b)(2), which states that an individual must undergo an employment history verification under § 1542.209 before gaining unescorted access to a SIDA. This paragraph would be changed to clarify that a criminal history records check is required pursuant to § 1542.209 rather than an employment history verification. This clarification would make the text of § 1542.205(b)(2) consistent with that of § 1542.209.

Finally, TSA proposes to add new paragraph 1542.205(c). This paragraph would make it clear 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 proposed § 1542.205.

The security measures required in a SIDA provide additional safeguards against unauthorized persons from gaining access to cargo operations where they could tamper with the cargo or stow away in attempt to take over the aircraft in flight, or introducing into cargo an unauthorized explosive, incendiary, or destructive substance or item.

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

Section 1544.101—Adoption and Implementation

The ASAC working groups recommended, and TSA agrees, that all-cargo aircraft operations conducted in aircraft with a maximum certificated take-off weight of more than 45,500 kg (100,309.3 pounds) should be subject to certain security requirements beyond those applicable to such operations under the current Twelve-Five Standard Security Program. TSA has already determined that this size aircraft is of a size that could cause significant damage if taken over and used as a weapon, and thus when this size aircraft is used in private charter passenger operations it must be operated under a private charter security program.[21] Additionally, the 45,500 kg threshold is consistent with international security standards adopted by the International Civil Aviation Organization. Accordingly, to ensure consistent treatment of similar aircraft, TSA proposes, in § 1544.101(h) and (i), to apply the same threshold by requiring that all-cargo operations in such aircraft be covered under an all-cargo program. Note that such aircraft carry both cargo and certain other persons (not passengers) in accordance with FAA rules. 14 CFR 121.547 and 121.583. These persons handle the cargo and perform other operations related to the flight.

Operations under an all-cargo program would no longer be under the current twelve-five program. Accordingly, TSA proposes to amend paragraph 1544.101(d)(1) to conform to the addition of the all-cargo program by providing that the twelve-five program does not apply for operations under an all-cargo program.

In addition, TSA proposes to change the requirement for a twelve-five program from aircraft with a maximum certificated takeoff weight ''of 12,500 pounds or more'' to ''more than 12,500 pounds.'' This section initially was based on the requirement in ATSA section 132(a) that TSA implement a security program for charter air carriers for aircraft having a maximum certificated takeoff weight of 12,500 pounds *or more.* In Vision 100, section 606(a), this was changed to require security programs for aircraft with a weight of *more than* 12,500.[22] This proposed amendment is consistent with Congressional intent. Vision 100 also codified the requirement for charter air carrier security programs in 49 U.S.C. 44903(l)(1).

Vision 100 section 606(a) also codifies in new 49 U.S.C. 44903(l)(2) an exemption for armed forces charters so they are not subject to the requirements of 44903(l)(1). Such military operations are not subject to the requirements of § 1544.101(d) or (e) and no TSA rule change is needed to implement this provision.

TSA also proposes to amend paragraph 1544.101(e)(1), which lists the elements of the twelve-five program. TSA proposes the following enhancements to the twelve-five program for all-cargo operations: § 1544.202 (Persons and property onboard the all-cargo aircraft) and § 1544.205(a), (b), and (d) (Acceptance and screening of cargo: Preventing or deterring the carriage of any explosive or incendiary, Screening and inspection of cargo, and Refusal to transport).

Section 1544.202—Persons and Property Onboard the All-Cargo Aircraft

Section 1544.201 currently requires passenger operations under full programs or private charter to screen, inspect, and provide other security for persons who board their aircraft and their accessible property. This section is geared largely to cover screening of passengers and their accessible property, though it also covers security measures for other persons boarding aircraft operated under full programs or private charter programs.

TSA proposes to add new § 1544.202. This section would require aircraft operators to apply the security measures in their security programs to persons who board the aircraft, and to their property. This proposed requirement is

[21] 67 FR 41635 (June 19, 2002), amended by 67 FR 79861 (Dec. 31, 2002).

[22] Century of Aviation Reauthorization Act, Pub. L. 108–176.

intended 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 would authorize TSA to incorporate into the security programs screening for unauthorized persons, or substances or items that could be used to pose a threat to transportation security.

TSA proposes to incorporate this requirement into both the twelve-five program for all-cargo operations and the proposed new all-cargo program. Such operators currently apply security measures to persons who board their aircraft under SDs that TSA has issued in response to threats. TSA envisions these measures to continue under this proposed rule.

Section 1544.205—Acceptance and Screening of Cargo

The ASAC working groups recommended, and TSA agrees, that security measures for and screening of air cargo should be enhanced. TSA proposes to amend paragraphs 1544.205(a), (b), (c), and (d) to broaden the scope of security measures that may be required in an aircraft operator security program, and to reference the Known Shipper program.

Specifically, TSA is proposing to require aircraft operators operating under a full, all-cargo, or twelve-five security program to inspect cargo for unauthorized persons, explosives, incendiaries, and other destructive substances or items. TSA believes that this amendment is necessary to prevent the introduction of stowaway hijackers, explosive devices, or other threats into air cargo. Carriers under these programs are currently required to inspect cargo to protect against such potential threats. This proposed provision would not alter that requirement but is adding it to the CFR and providing industry an opportunity for public comment. The security measures in proposed § 1544.205(a) and (b) are the same as those incorporated into SDs that have been issued and are currently being carried out by aircraft operators with full programs and twelve-five programs.

Proposed § 1544.205(b) would authorize TSA to incorporate into an aircraft operator's security program screening of cargo for unauthorized persons, or substances or items the intentional misuse of which could pose a threat to transportation security.

Current § 1544.205(c) provides that the aircraft operator must prevent access by persons other than an aircraft operator employee or its agent. TSA is proposing to add that persons authorized by the airport operator or host government also may have access. Such individuals as Customs inspectors and airport law enforcement officers must have access to such areas.

TSA also proposes to strengthen the cargo acceptance requirements applicable to aircraft operators operating under a full program or an all-cargo program. Pursuant to proposed § 1544.205(e), an aircraft operator would be permitted to accept cargo for air transportation only from entities that have comparable security programs. TSA believes that this provision is necessary to secure the aircraft by strengthening the integrity of the air cargo supply chain. These requirements parallel those currently applied to operations conducted under a full program.

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

Section 1544.225—Security of Aircraft and Facilities

The ASAC working groups recommended, and TSA agrees, that additional steps should be taken to assure that attempted unauthorized access to the aircraft and cargo is detected and prevented.

Proposed paragraph 1544.225(d) would require the operators of aircraft operating under a full program or an all-cargo program to prevent unauthorized access to the operational area of the aircraft while loading or unloading cargo. This requirement would apply to operations conducted both within and outside a SIDA. TSA recognizes that current paragraph 1544.225(b) requires all aircraft operators operating under security programs to prevent unauthorized access to each aircraft. Proposed paragraph (d) would broaden this requirement, for aircraft operated under a full or an all-cargo program, to clarify that unauthorized access must be prevented to the operational area around the aircraft during cargo loading and unloading operations. This measure would provide an additional layer of protection around the aircraft.

Section 1544.228—Security Threat Assessments for Cargo Personnel

TSA proposes to require persons who have unescorted access to cargo to undergo a security check. This would require that they comply with the requirements of subpart C of part 1540 by successfully completing a Security Threat Assessment, or that they undergo a criminal history records check under current rules, or other approved Security Threat Assessment. This requirement would apply to aircraft operators under a full program or an all-cargo program.

TSA believes that this step is necessary to reduce the likelihood of a terrorist gaining employment in a position with access to cargo for the purpose of introducing an explosive, stowaway hijacker, or other destructive substance into air cargo. Extending Security Threat Assessments to these individuals would allow for a comparable degree of security for all personnel with access to cargo on behalf of regulated parties from the time it is picked up from a shipper to the time it is loaded on the aircraft.

This proposal would allow for another Security Threat Assessment to be approved by TSA. For instance, if the individual had undergone a Security Threat Assessment for the issuance of a hazardous materials endorsement on a commercial drivers license in accordance with 49 CFR 1572.5, TSA could approve that as acceptable for compliance with proposed § 1544.228.

TSA has proposed a fee structure and collection process to fund some or all of the costs associated with the proposed Security Threat Assessment requirements. The proposed fee may be found at section VII titled Fee Authority for the Security Threat Assessment of this NPRM.

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

The ASAC working groups recommended, and TSA agrees, that the identities of persons who perform certain key actions with air cargo should be subject to verification and that the backgrounds of these persons should be checked. TSA proposes to broaden the background check requirements by revising paragraph 1544.229(a)(1)(iii)(B) to include a cross-reference to the new paragraph 1544.229(a)(1)(iii)(C). The new paragraph requires persons who screen cargo that will be carried on an aircraft of an operator required to screen cargo under part 1544 to submit to a CHRC under § 1544.229. Currently, § 1544.229 applies, in pertinent part, only to persons having authority to screen cargo, in the United States, of an

aircraft operator required to screen passengers under this part, or serving as an immediate supervisor of such an individual, when the cargo will be carried in the cabin of the aircraft. Accordingly, only cargo screeners for operators with full programs currently are subject to § 1544.229. This new requirement parallels the current requirement that persons who screen passengers and carry-on baggage (accessible property) must comply with § 1544.229. TSA also proposes to require that cargo screeners for operators with all-cargo programs be subject to the criminal history records check requirements of § 1544.229. This change would provide an additional protection against individuals who screen cargo for the largest all-cargo aircraft from using their positions to introduce unauthorized explosives, incendiaries, persons, or destructive substances or items into the cargo or aircraft.

Section 1544.239—Known Shipper Program

Proposed § 1544.239 would codify 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 United States Congress as a form of screening in ATSA. Aircraft operators operating under a full program would be 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 would apply to operations under full programs.

Aircraft operators with full programs are already required to maintain a Known Shipper program under their security programs. TSA believes that it is prudent to set out the major features of this program in regulation at this time. Additional changes to how the Known Shipper program must operate may be included in revisions to the security program.

Part 1546—Foreign Air Carrier Security

Section 1546.101—Adoption and Implementation

The ASAC working groups recommended, and TSA agrees, that cargo operations of foreign air carriers that land or take-off in the United States should be required to conform to essentially the same requirements as those applicable to comparable operations by domestic aircraft operators. TSA proposes to broaden 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. TSA proposes to establish the requirements of an appropriate security program for a covered foreign air carrier conducting all-cargo operations for operations in aircraft having a maximum certificated take-off weight greater than 45,500 kg (100,309.3 pounds) (analogous to a U.S. all-cargo program under part 1544), and for operations in aircraft having a maximum certificated take-off weight greater than 12,500 pounds up to 45,500 kg (100,309.3 pounds) (analogous to a U.S. twelve-five program in all-cargo operations under part 1544).

Section 1546.103—Form, Content, and Availability of Security Program

TSA proposes to make an administrative change to paragraph 1546.103(a) by removing the word ''passenger'' and changing ''U.S. air carriers'' to ''U.S. aircraft operators.''

In paragraph 1546.103(b), TSA proposes to add paragraphs 1546.101 (e) and (f) to the introductory text. This proposed change broadens the requirements to embrace cargo operations.

Section 1546.202—Persons and Property Onboard the Airplane

This proposed new section parallels the requirements of the proposed aircraft operations in the United States. The rationale for this addition is described in the section-by-section analysis for § 1544.202.

Section 1546.205—Acceptance and Screening of Cargo

The ASAC Working groups recommended, and TSA agrees, that, consistent with recognition of the sovereignty of foreign states, aviation security regulations should be clarified with respect to the duty of foreign air carriers for the security of air cargo loaded in or destined for the United States. TSA proposes to amend paragraph (a) and add paragraphs (c), (d), (e), and (f) to § 1546.205. These paragraphs are parallel to those for U.S. aircraft operators in proposed § 1544.205.

Proposed paragraph 1546.205(d), ''Screening and inspection of cargo in the United States,'' would provide that each foreign air carrier must ensure that, as required in its security program, cargo is screened and inspected for explosives, incendiaries, unauthorized persons, 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.

Proposed paragraph 1546.205(e), ''Acceptance of cargo in the United States,'' would provide 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.

Proposed paragraph 1546.205(f) would provide 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

TSA proposes to require persons who are not required to complete a CHRC under §§ 1542.209, 1544.229, or 1544.230 and who have unescorted access to cargo, to comply with the requirements of subpart C of part 1540 by successfully completing a Security Threat Assessment. This requirement would apply to foreign air carriers under paragraphs 1546.101(a), (b), or (e). The rationale for this security measure parallels that rationale described in the section-by-section analysis for § 1544.228.

Section 1546.215—Known Shipper Program

TSA proposes to codify the Known Shipper program for the foreign air carriers just as we proposed in § 1544.239. The rationale for adding this new section is the same as stated in the section-by-section analysis for § 1544.239.

Part 1548—Indirect Air Carrier Security

Section 1548.5—Adoption and Implementation of the Security Program

TSA proposes to revise paragraphs (a), (b), and (c) of § 1548.5 regarding the adoption and implementation of the

IACSSP. The proposed change to paragraph 1548.5(a) would specify that no IAC may offer cargo to an aircraft operator operating under a full program or an all-cargo program specified in part 1544, or to a foreign air carrier operating a passenger operation under paragraphs 1546.101(a) and (b) or an all-cargo program under paragraph 1546.101(e), unless that IAC has and carries out an approved security program under part 1548.

The proposed change to paragraph 1548.5(b) would broaden the scope of screening actions that may be required in an individual IAC's security program. IACs 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.'' TSA proposes to revise this requirement to provide that the IAC must ''provide for the security of persons and property traveling in air transportation against acts of criminal violence and air piracy and the introduction of any unauthorized person, explosive, incendiary, or other destructive substances or items as provided in the IAC's security program.''

This provision would also broaden the duty of IACs to include cargo to be carried on an aircraft operated under an all-cargo program rather than solely in passenger operations. This change parallels the cargo security requirements in proposed §§ 1544.205 and 1546.205. It authorizes TSA to incorporate into an IAC's individual security program screening of cargo for unauthorized persons, or substances or items the intentional misuse of which could pose a threat to transportation security. Under § 1548.5(b)(1)(i), this requirement would apply from the time the IAC accepts the cargo to the time it transfers the cargo to an entity that is not an employee, agent, contractor, or subcontractor of the IAC. This proposed provision clarifies the existing IAC security program requirement that the IAC is responsible for carrying out security measures under this part when its employee, agent, contractor or subcontractor fulfills its function. Section 1548.5(b)(1)(ii) would apply while the cargo is stored, en route, or otherwise being handled by an employee, agent, contractor, or subcontractor of the IAC. Section 1548.5(b)(1)(iii) would apply regardless of whether the IAC has or ever has physical possession of the cargo. At times, IACs perform cargo services that may include arranging for transportation of cargo by other entities. This proposed amendment clarifies that the IAC is responsible for these shipments even though the IAC, itself, does not have physical possession. Proposed paragraph 1548.5(b) would also require the IAC to assure that its employees, agents, contractors, and subcontractors comply with the requirements of the IAC's security program. This provision currently is in the IACs' standard security programs.

The proposed change to paragraph 1548.5(c) would assure that the content of each IAC security program reflects the scope of security measures established under proposed § 1548.5(b), references Known Shipper program requirements that are proposed to be codified in § 1548.17, and establishes a new requirement that each IAC security program include documentation of the procedures and curriculum used to accomplish the training of persons who accept, store, transport or deliver cargo for or on behalf of the IAC. This training would be required under proposed new § 1548.11.

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

TSA proposes to restructure and revise this section both to reflect actual practices and enhance the security of this regulatory regime. The proposed revision of paragraph 1548.7(a) accounts for the fact that TSA has developed the IACSSP. Consistent with current practices, rather than submitting a security program for TSA approval, an entity would request approval to operate under the IACSSP. The proposed addition 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 1548.7(a) also proposes the process that TSA will follow to approve an applicant's operation under a security program, proposes that approvals would be effective for one year, and provides that the approved IAC must notify TSA of changes to the initial application. TSA would use the information submitted by IAC applicants to verify their legitimacy through a check of publicly-available records and to cross check that information against data on known and suspected terrorists.

Under current practices, TSA issues an IACSSP to expire each year. The proposed addition of paragraph 1548.7(b) presents the processes an IAC must follow to annually seek renewed TSA approval to operate under the IACSSP. Annual renewal would be a continuation, and codification, of the current practice. Other entities regulated by a TSA security program, such as aircraft operators and airports, must obtain FAA certification. IACs are not required to do so. Additionally, TSA has found that the IAC industry has a high degree of turnover. Accordingly, TSA proposes in paragraph 1548.7(b) that the IAC must submit to TSA for renewal at least 30 calendar days prior to expiration of the IACSSP as well as other standards for the submission. The proposed renewal standards also include that the IAC certify that it has provided TSA with its most up-to-date information and acknowledge that intentional falsification of the information may be subject to civil and criminal penalties. The addition further proposes the standard for TSA to renew the approval of an IACSSP. Proposed § 1548.7(b) otherwise codifies the existing security program required for annual renewal.

The proposed additions of paragraphs 1548.7(c), (d), and (e) revise the existing requirements of paragraphs 1548.7(b), (c) and (d), respectively. Many of the changes parallel changes made previously to similar requirements for airport operator security programs and aircraft operator security programs in §§ 1542.105 and 1544.105. In part, the new paragraphs have been moved to ensure that the structure of the section remains logical. Proposed § 1548.7(c) closely parallels the existing § 1548.7(b), but adds § 1548.7(c)(6)—allowing a group of IACs to submit a proposed amendment together. Proposed paragraph 1548.7(d) is the same as the existing paragraph 1548.7(c). The proposed paragraph 1548.7(e) revises the existing Emergency Amendments (EA) standards of the existing paragraph 1548.7(d). The proposed paragraph is separated into three subparagraphs for easier reading. Proposed paragraph 1548.7(d)(1) substitutes ''aviation security'' for ''safety in air transportation or in air commerce'' to clarify the breadth of TSA's EA authority. Proposed paragraph 1548.7(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 1548.7(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.

TSA proposes to codify procedures for TSA to withdraw an IAC's approval to operate under the IACSSP with the

addition of paragraph 1548.7(f). The proposed standard for withdrawal is a TSA determination that the operation is contrary to security and the public interest. Proposed paragraph 1548.7(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 proposes the codification of emergency withdrawal procedures. This proposal creates procedural guidelines to implement withdrawal of a security program and affords due process to the IAC. The emergency procedures would allow the IAC to submit a petition for reconsideration, but the filing of a petition will not stay the effective date of withdrawal.

Proposed paragraph 1548.7(g) adds provisions for proper service of documents in the withdrawal proceedings. Procedures for time extensions are proposed at paragraph 1548.7(h).

Section 1548.9—Acceptance of Cargo

TSA proposes to revise paragraph 1548.9(a) to broaden the scope of the IAC's duty to prevent or deter the carriage of unauthorized persons or destructive substances or items on board an aircraft to the existing requirements regarding explosives and incendiaries. With the expanded definition of IAC, this provision proposes to require IACs to carry out these procedures whenever offering cargo for air transportation on all-cargo aircraft, as well as a passenger aircraft under a full program. This proposed section further provides that, subject to TSA approval of the provisions of the IAC's security program. Additionally the proposed amendment would add a requirement that the IAC request the shipper's consent to search or inspect the cargo.

TSA proposes to revise paragraph 1548.9(b) by adding all-cargo aircraft operations to the search and inspection requirements. Under current paragraph 1548.9(b), this duty extends only to cargo that is intended for shipment aboard a passenger aircraft. By removing the word ''passenger,'' this paragraph would extend to cargo for shipment aboard all-cargo aircraft operations as well. Proposed paragraph 1548.9(b) would delete the requirement, found in current paragraph 1548.9(b), that the IAC must search or inspect cargo. This amendment is primarily aimed at creating a parallel structure to the requirements found in parts 1544 and 1546.

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

The ASAC working groups recommended, and TSA agrees, that certain employees of IACs, and of agents, contractors, and subcontractors performing services for IACs, should be subject to security-related training. These enhanced requirements for training covers individuals who perform security-related duties to ensure the appropriate security standards are met.

TSA proposes to add new § 1548.11(a), which 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 would cover employees of the IAC as well as employees of any agent, contractor, or subcontractor performing security-related duties for the IAC.

Under proposed § 1548.11(b), additional training would be 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 SDs 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.

Proposed paragraph 1548.11(c) would require annual recurrent training of covered individuals in these elements of knowledge. Pursuant to proposed § 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.

Section 1548.13—Security Coordinators

The ASAC working groups recommended, and TSA agrees, that communication among regulated aircraft operators, airport operators, TSA, and IACs concerning security matters must be improved, and responsibility for compliance by IACs with TSA security requirements must be clarified. TSA proposes to require each IAC to designate and use an Indirect Air Carrier Security Coordinator (IACSC). The IAC would be required to appoint the IACSC at the corporate level, and IACSC would be directed to serve as 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 would be required to be available on a 24-hour basis. This proposed 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

The ASAC working groups recommended, and TSA agrees, that the identities of personnel who have unescorted access to cargo to be shipped by air should be verified, and that such personnel should be subject to an appropriate background check. TSA proposes to add new § 1548.15, which would prohibit each IAC from authorizing any individual unescorted access to cargo until the IAC has verified the identity of that individual in a manner acceptable to TSA, and that individual has successfully completed a Security Threat Assessment pursuant to proposed subpart C of 1540. The rationale for this security measure parallels that described in the section-by-section analysis for § 1544.228.

Section 1548.17—Known Shipper Program

TSA proposes to add new § 1548.17 to codify 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

The ASAC working groups recommended, and TSA agrees, that communication between regulated IACs and TSA concerning security matters must be improved, and responsibility for compliance by IACs with TSA security requirements must be clarified. In the past, when threat conditions required that additional security measures be carried out immediately, TSA has issued EAs to IACs' security programs. This section would, in part, provide a procedure for TSA to impose such measures using SDs. TSA proposes to add new § 1548.19, which would authorize TSA to issue SDs and Information Circulars to regulated IACs, and would mandate compliance by the IAC with each SD that it receives. Proposed § 1548.19 would also require 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 an SD, proposed § 1548.19 would authorize

the IAC to submit proposed alternative measures and the basis for the alternative measures to TSA for approval. The IAC would be required to submit the proposed alternative measures within the time prescribed in the SD and, if they are approved by TSA, the IAC would be required to implement them.

Proposed § 1548.19 also provides that each IAC that receives an 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. Proposed § 1548.19 also provides that submission of a comment would not delay the effective date of the SD.

Proposed § 1548.19 also provides that each IAC that receives a SD or Information Circular and each person who receives information from a SD or Information Circular would be required to restrict the availability of the SD or Information Circular, and information contained in either document, to those persons with a need-to-know. The IAC would be required to refuse to release the SD 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.

VI. Proposed Compliance Schedule

Most of the provisions in this proposed rule would codify existing SD requirements. It appears to TSA that most of the new provisions in this proposed rule are achievable by the regulated parties within 90 days. However, TSA recognizes the need for further time to implement some provisions. TSA proposes that the proposed rule, if adopted, would become effective as follows:

(1) The proposed rule would become effective 90 days after the date of publication of the final rule in the **Federal Register** and operators would generally be required to comply with the requirements (with the exception of the compliance date described in VI. (2)).

(2) TSA proposes that certain measures in the proposed rule would require compliance by 180 days from the date of publication of the final rule in the **Federal Register**. TSA believes IACs will need as much as 180 days to introduce new training requirements under § 1548.11 and to establish and operate under a TSA security program pursuant to § 1548.7. Finally, TSA proposes to provide 180 days for aircraft operators, foreign air carriers, and IACs to comply with the security threat assessment for those individuals required to submit to the requirements pursuant to proposed §§ 1544.228, 1546.213, and 1548.15.

TSA requests additional information from the public on how many operators would be affected, what the impact would be on those individual operators, and the proposed compliance schedule.

VII. Fee Authority for Security Threat Assessment

The USA PATRIOT Act did not grant TSA authority to collect fees to cover the costs associated with completing background checks. However, 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, including implementation of the USA PATRIOT Act requirements.[23] Fees collected under this legislation (Section 520) must 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 the background records check or providing the 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 the background check or providing the credential. The fee shall remain available until expended. TSA is establishing this fee in accordance with the criteria 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 handling cargo is very large and that extending fingerprint-based records checks to 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 is proposing a focused Security Threat Assessment program to determine whether individuals seeking to handle cargo present a terrorist threat. This program will reduce the likelihood that a terrorist might gain access to a cargo aircraft.

Flexibility will be achieved by ensuring that each of the following individuals with unescorted access to cargo be required to have either a Security Threat Assessment or unescorted SIDA access: (1) IAC personnel; (2) Aircraft Operator personnel operating under a full program or an all-cargo program; and (3) Foreign Air Carrier personnel under 49 CFR 1546.101(a), (b), or (e). TSA also proposes to conduct a Security Threat Assessment on each officer, director and person who holds 25 percent or more of total outstanding voting stock of an Indirect Air Carrier or entity applying to become an IAC.

Security Threat Assessment Population

Personnel with unescorted access to cargo that work for an IAC, an aircraft operator, or a foreign air carrier would be required to undergo a name-based Security Threat Assessment. Additionally each officer, director and person who holds 25 percent or more of total outstanding voting stock of an Indirect Air Carrier or entity applying to become an IAC would be required to undergo a name-based Security Threat Assessment. TSA approximates a *de minimis* number of persons who hold 25 percent or more total outstanding voting stock that are not also officers or directors of these IACs. Accordingly, TSA has not accounted for these individuals separately. However, those personnel with unescorted SIDA access have undergone a criminal history records check. TSA would accept the criminal history records check in lieu of the proposed Security Threat Assessment for these personnel.

The Indirect Air Carrier Population

TSA estimates that there are approximately 3,800 companies that are defined as IACs. TSA further estimates that there are approximately 7 employees per IAC. Therefore the total population is estimated to be 26,600.

[23] Department of Homeland Security Appropriations Act, 2004, Section 520, Pub. L. 108–90, October 1, 2003, 117 Stat. 1137.

Cargo Personnel Not Subject to Other TSA Security Threat Assessments

TSA has 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 Security Threat Assessment. As discussed in the economic evaluation, aircraft operators and foreign air carriers have some employees who are required to submit to the fingerprint-based SIDA check but some employees would only be required to submit to the Security Threat Assessment. Because most of the operator employees are covered in the SIDA background check requirements, TSA believes that only a limited number of employees would be required to submit to a Security Threat Assessment and not the security assessment for SIDA workers. There may be instances where all employees with access to the cargo will have the security assessment for SIDA workers. TSA estimates that there are approximately 25 employees for each aircraft operator and foreign air carrier operating all-cargo flights who would be required to submit to a Security Threat Assessment. Therefore the total population is estimated to be 1,625 (65x25).

Total Initial Population

Given the IAC population of 26,600 and the population of relevant aircraft operators and foreign air carriers operating all-cargo flights employees of 1,625, the total population subject to a Security Threat Assessment is 28,225 (26,600 + 1,625). This initial population would be required to submit to a Security Threat Assessment during the first year of the program.

Recurring Population

TSA estimates approximately 15% of the initial total population would be required to submit to a Security Threat Assessment each year after the initial assessment. This percentage represents new employees or employees with a new requirement for the Security Threat Assessment. Therefore the recurring population that would be required to submit to a Security Threat Assessments is estimated to be 4,234.

Five Year Population

Given the first year population of 28,225 and subsequent annual recurring population of 4,234, we estimate that the total population receiving a Security Threat Assessment over the first 5 years is 45,161 (28,225 + 4 × 4,234).

Program Costs

This section summarizes TSA's estimated costs for establishing the program, processes, and resources to establish and perform the Security Threat Assessment on the appropriate population.

Leveraging Existing Resources

Where possible, TSA would leverage existing processes, infrastructure and personnel that are envisioned to be in place for other Security Threat Assessment programs at the time this program on Security Threat Assessment begins operation. Existing infrastructure that would be leveraged include the HAZMAT Endorsement Program's [24] Hazardous Materials Endorsement Screening Gateway System (HMESG); however, some modifications to these systems would be necessary to meet proposed requirements. These changes would include connectivity with additional government agencies, software enhancement and additional backup capabilities. In addition to the HMESG, this program would leverage existing real estate and Project Management Office personnel. The additional costs that would be incurred by the HAZMAT program have been identified in the recurring cost section below.

Start-Up Costs

We estimate that the total start-up costs would be $690,000. This includes $570,000 for hardware and software modifications for the existing HAZMAT HMESG and $120,000 for program management personnel. See Figure 1 below for additional details.

Recurring Costs

We estimate that the total annual recurring costs would be $928,354 for the first year and $214,102 for each subsequent year. These costs include an annual $50,000 expense TSA will incur for connectivity and $66,454 expense for use of the HAZMAT program infrastructure. The use of the HAZMAT program infrastructure would include use of program management, adjudication and fee processing personnel, use of real estate, and use of systems. The first recurring year would have significantly higher costs associated with those costs that are completely variable (*i.e.*, a function of the number of Security Threat Assessments performed). The combined first year cost for third party terrorist threat [25] checks and third party clearinghouse fees will be $783,675 and the costs for the four following years would be $93,414 annually.

FIGURE 1.—COSTS ESTIMATES

Category and subcategory	Description	Start-Up	Year 1	Recurring
Hardware/Software:				
HAZMAT HMESG Modification	The Hazardous Materials Endorsement Screening Gateway System.	$570,000		
HAZMAT HMESG Connectivity			$50,000	$50,000
Hardware/Software Total		570,000	50,000	50,000
Federal Personnel: Personnel to staff program office.	Additional federal employees will be required to staff the program office during the start-up phase. In the start-up phase, one FTE at $120,000 annually will be necessary for program implementation and development.	120,000		
Total Federal Personnel		120,000		

[24] The HAZMAT Endorsement Program is a program currently being developed by the TSA to provide background checks on drivers with a Hazardous Materials Endorsement on their Commercial Drivers License. Initially, all current endorsement holders will have a name-based check performed on them and, as an individual renews or applies for a HAZMAT endorsement, a fingerprint-based background check will be performed.

[25] The third party assessments include (i) those performed by the Office of National Risk Assessment (ONRA) and (ii) FBI named-based checks through Automated Case Systems (ACS).

FIGURE 1.—COSTS ESTIMATES—Continued

Category and subcategory	Description	Start-Up	Year 1	Recurring
Third Party Clearinghouse Fee: Third Party Clearinghouse Fee.	The third party clearinghouse will collect and process the applicant's biographical information, collect the applicant fee and forward the information and fee to TSA.	.....	84,675	12,702
Total Third Party Clearinghouse Fee	.....	.....	84,675	12,702
Terrorist Threat Assessment:				
Automated Case System Fee (FBI name based checks-Automated Case Systems).	A terrorist threat analysis is the process of querying applicant names in terrorist threat and criminal databases. This cost is derived by multiplying the total population by the cost per applicant of several database checks. $20 per applicant.	.....	564,500	67,260
Office of National Risk Assessment Fee	A terrorist threat analysis is the process of querying applicant names in terrorist threat and criminal databases. The cost is derived by multiplying the total population by the cost per applicant of several database checks: $4 per applicant.	.....	134,500	13,452
Total-Terrorist Threat Assessment	.....	.....	699,000	80,712
Additional costs to existing programs: Additional costs incurred by HAZMAT program.	Leveraging the planned infrastructure to the HAZMAT program will increase the total recurring costs by 1% per year. The cost here is 1% of the average relevant annual costs. Includes Federal and Contractor personnel, Office Facilities, and Systems.	.....	66,454	66,454
Total additional costs to existing programs	.....	.....	66,454	66,454
Total Costs	.....	690,000	928,354	214,102

Total Costs

Based on its population and cost estimate assumptions, TSA estimates that start-up phase costs would be approximately $690,000 and recurring phase costs would be approximately $928,354 annual for the first recurring year and $214,102 for each subsequent year. Therefore the total cost of the program for the first 5 years would be $2,474,762.

Cost Adjustments

Pursuant to the Chief Financial Officers Act of 1990, DHS/TSA will review this fee at least every two years.[26] Upon review, if it is found that the fee is either too high or too low, a new fee will be proposed.

Fee Calculation

TSA is proposing to charge a fee to cover the recurring costs of the program. Start-up costs will be provided by TSA.

Recurring Phase Costs

TSA estimates that the total annual recurring phase costs for the first 5 years would be $1,784,762. These total costs consist of the sum of the first year costs plus the four recurring years at $214,102 per year. The expected applicants divide these costs over the first 5 years. Therefore the fee associated will be $39 ($1,784,762/45,161) per applicant, rounded to the nearest dollar from $39.52. The fees are based on summing the annual costs and population over 5 years. This calculation is done in order to account for any variability that may arise from the imprecise nature of the population and cost estimates.

Fee Remittance Process

TSA would employ a third party to establish the infrastructure for collecting data and fees, cleansing data, and forwarding the funds and information to TSA. This process would function in a similar manner to other TSA background check programs and may include the services of Pay.gov. The third party processing costs are accounted for in the ''Third Part Clearinghouse Fee'' category in Figure 1–Cost Estimates.

VIII. Regulatory Evaluation Summary

Proposed 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 (Public Law 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 proposed rule:

(1) Has benefits which are likely to justify its costs, is not a ''significant regulatory action'' as defined in the Executive Order, but is significant due to public interest, rather than economically;

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

[26] 31 U.S.C. 902.

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

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

These analyses, available in the docket, are summarized below.

Economic Impacts

This summary highlights the costs and benefits of the proposed rule to amend the transportation security regulations to further enhance and improve the security of air cargo transportation. TSA has determined that this is not a major rule within the definition of Executive Order 12866, as annual costs or benefits to all parties do not pass the $100 million threshold in any year. Likewise there are no significant economic impacts for each of the required analyses of small business impact, international trade, or unfunded mandates. A separate detailed regulatory evaluation is available in the docket and TSA invites comments on all aspects of the economic analysis.

TSA proposes to create a mandatory security program for all-cargo aircraft operations over 45,500 kg (100,309.3 lbs) and to amend existing security regulations and programs for aircraft operators, foreign air carriers, airport operators, and IACs. IAC would be redefined to include those transporting goods via all-cargo aircraft. Mandatory security programs for all-cargo operations would replace the voluntary DSIP and extensively build on the requirements of the Twelve-Five Standard Security Program. TSA also proposes to expand the use of background checks and threat assessments to new populations, including IAC employees and individuals who have unescorted access to cargo, where such operations are either outside of the currently defined airport SIDA.

Costs

The following sections summarize the estimated costs of this NPRM by general category of who pays. A summary table is provided for an overview of the cost items, the regulation section creating the requirement, and a brief description of cost elements. Both in this summary and the economic evaluation, descriptive language is used to address the consequences of the regulation. Although the regulatory evaluation attempts to mirror the terms and wording of the regulation, no attempt is made to replicate precisely the regulatory language and readers are cautioned that the actual regulatory text, not the text of the regulatory evaluation, is binding.

Aircraft Operators will incur additional costs to comply with requirements of this NPRM. Over the 10-year period of 2004–2013, all-cargo aircraft operators are estimated to incur costs totaling approximately $600,000 to comply with new requirements to require background checks for individuals who screen cargo for all-cargo airplanes and their supervisors, as well as for employees with unescorted access to the cargo. The NPRM proposes to require all-cargo aircraft operators to screen all persons entering the aircraft. This requirement is estimated to impose additional costs of approximately $33.7 million over the ten-year period of this analysis. All-cargo aircraft operators also will be required to take additional measures to secure the aircraft and facilities at an estimated cost of $33.6 million. Although every all-cargo operator will now have to designate a security coordinator, many already have the requirement. The estimated cost for these duties is $200,000. All-cargo aircraft operators who conduct operations with airplanes having a maximum certificated take-off weight greater than 45,500kg (100,309.3 lbs) would be required to provide additional law enforcement capability to comply with proposed requirements to extend or create new secure areas to encompass air cargo operations. TSA estimates this ten-year cost to be $27 million. Finally, proposals to require random screening of cargo on passenger aircraft and on all-cargo flights are estimated to impose additional ten-year costs of $493 million, and $167 million, respectively.

Airport Operators of airports that currently have one or more SIDAs will be required to extend or create a new SIDA to encompass air cargo operations. This proposed change would apply only to aircraft operations conducted with airplanes having a maximum certificated take-off weight greater than 45,500kg (100,309.3 lbs) operating a full or all-cargo program. TSA estimates the cost of this requirement to be $900,000 over the ten-year period of this analysis. This cost reflects the cost of additional employee badges, and the administrative costs of updating the airports' security plans.

Indirect Air Carriers will be impacted in several ways if the proposals in this NPRM become effective. IACs will be required to complete Security Threat Assessments for individuals having unescorted access to cargo. This requirement is estimated to impose costs totaling $3.4 million over ten years. IACs also will be 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 $15.1 million over the ten-year period 2004–2013. These costs include the cost of initial training and annual recurrent training for the IAC labor force. This NPRM 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 $36 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 were not estimated separately from domestic carrier costs; a separate discussion for these costs is not included. This method of cost consideration reflects the way DOT reports 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.

TSA will incur costs as a result of the proposed rule. To develop the training that IACs will be required to implement and ensure that IAC employees have completed will cost the agency approximately $450,000. TSA also will incur costs to administer the Known Shipper program of approximately $24.5 million. The cost to TSA for the vetting of IACs is estimated at $2.6 million. TSA will also be modifying a system under development for another rule to accommodate the Security Threat Assessments in this proposed rule. The costs of utilizing this system are included in a fee proposal and therefore are captured in the unit costs used to develop the costs for the aircraft operators and IACs.

In summary, the cost impacts of this NPRM are estimated to total approximately $837 million, undiscounted, over the period 2004–2013. Aircraft operators will incur costs totaling $758 million; airport operators $900,000; IACs $51 million; and TSA anticipates cost expenditures to administer the provisions of the NPRM at $28 million over the ten year analysis period. Details on how estimates were developed, as well as the discounted value comparisons, are included in the full regulatory evaluation. The following table summarizes the estimated costs.

BILLING CODE 4910–62–P

TEN-YEAR UNDISCOUNTED COST SUMMARY

Ten-Year Costs (Undiscounted, Millions of Constant 2003 Dollars)

Section	Who \ Year	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	Total*
1540.; 1548.15; 1544.228	Expand security threat assesments for IAC employees w/unescorted access to cargo and U.S. air carrier employees w/access to cargo but have not had a CHRC.	2.1	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.2	3.7
1542.205	Extend SIDA to all-cargo areas.	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.9
1544.229	(all cargo) Expand background check requirements to individuals who screen cargo for all-cargo planes with unescorted access to cargo in the SIDA and new ID requirements.	0.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5
1544.101	Implement all-cargo AO std sec program (for all-cargo operations and operations >45.5kg).	2.7	2.7	2.7	2.7	2.7	2.7	2.7	2.7	2.7	2.7	26.6
1544.101; 1544.202	Require all-cargo AO to screen all persons entering the aircraft (new for all-cargo AO and upgrades 12.5 program).	3.0	2.9	3.0	3.1	3.3	3.4	3.5	3.7	3.9	4.0	33.7
1544.101; 1544.225	New requirements for inspecting the aircraft (tampering, items not belonging).	2.4	2.6	2.9	3.1	3.4	3.7	4.0	4.4	4.8	5.2	36.6
1544.101; 1544.215; 1544.305	Require that all-cargo AO designate security coordinators.	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2
1544.205	Passenger Flight Cargo Screening	56.2	56.1	59.1	46.0	46.0	46.0	46.0	46.0	46.0	46.0	493.1
1544.205	All-Cargo Flight Cargo Screening	18.8	18.7	20.9	15.4	15.4	15.4	15.4	15.4	15.4	15.4	166.4
1546	Foreign Air Carriers	(FAA data doesn't separate data by carrier registration, so foreign flag carrier cost in U.S. is reflected in other detail lines. Costs incurred overseas will be similar to those of domestic carriers)										
1544.239; 1546.215; 1548.17	TSA-managed web-based Known Shipper Database.	2.9	2.4	2.4	2.4	2.4	2.4	2.4	2.4	2.4	2.4	24.5
1548.11	Develop and implement an IAC and Agent training (on pax acft). Develop a TSA testing tool.	3.1	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	15.1
1548.7	IAC security program requirements	4.2	3.7	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5	36.0
	Total*	95.7	90.8	96.1	77.8	78.2	78.7	79.2	79.7	80.3	80.9	837.3

***Note: Totals may not sum due to rounding.**

<FNP>

Benefits

The primary benefit of the proposed rule would be increased protection to persons and property in the U.S. from acts of terrorism; however, some aspects of this proposed rule would provide

cost savings for the industry as well. This NPRM is intended to enhance and improve the security of air cargo transportation. The proposed rule is designed to prevent unauthorized persons, explosives, incendiaries, and other substances or items from being introduced into the air cargo supply chain. Persons on the ground, in buildings, and elsewhere in our society would also be afforded enhanced protection against acts of terrorism involving the use of an all-cargo aircraft.

The warning late in 2003 from U.S. Intelligence sources was swift and simple: terrorists are considering using cargo aircraft—freighters that carry mostly boxes instead of people. Homeland Security officials recently declared the existence of intelligence that indicated al-Qaeda may be plotting an attack using cargo planes. One security conscious carrier has petitioned the U.S. government to allow checks on people with access to cargo planes.[27]

Strengthening air cargo security and expanding security measures to all-cargo aircraft operations would provide important countermeasures against possible terrorist activities aimed at ultimately destroying commercial passenger aircraft and all-cargo aircraft in flight. Provisions of the NPRM also reduce the opportunity for terrorists to use aircraft involved in the transport of cargo to achieve their goals.

Although it is difficult to impossible to project statistically the likelihood of incidents of terrorist acts involving aircraft, the following table reports the costs of several significant events that give examples of the potential impact of terrorism to civil aviation:

EXAMPLES OF INCIDENTS

Year	Event	Type of attack	Property loss	Loss of life/bodily injury	Total cost
1986	Pan Am 073	Aircraft hijacking	$0.55M	$66M death $72.5M injury	$139.05M
1987	Korean Airlines 858	Mid-air explosion		$345M	
1988	Pan Am 103	Mid-air explosion	$184M	$810M	$994M
2001	New York World Trade Center.	Aircraft used as a weapon			$16B[28]

[28] The General Accounting Office (Review of Studies of the Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center, GAO–02–700R, May 29, 2002) reviewed 8 separate studies that estimated the impact of the 9/11 destruction of the World Trade Center. Their conclusion was that the best estimate of un-reimbursed cost was $16 billion.

Following significant security incidents, such as those reported in the table titled ''Examples of Incidents,'' security agencies have strengthened measures designed to prevent recurrences. For this reason, the full benefits of avoiding losses such as those presented in the table are not claimed in this NPRM. However, terrorist events continue to be threatened. Moreover, it appears that the use of a large commercial aircraft as a weapon, unprecedented prior to September 11, 2001, has the potential to raise the cost of a terrorist event by an order of magnitude. (The table titled ''Example of Incidents'' does not reflect the additional costs of investigations, government action, and loss of business due to decreased passenger levels. Consideration of these costs would increase the cost of a successful terrorist event beyond the numbers presented in the table titled ''Example of Incidents.'' Against this scale, it is clear that avoiding just one incident of the magnitude that has been characteristic of the types of terrorist acts this proposed rule is intended to protect against more than justifies the costs imposed by this NPRM.)

Initial Regulatory Flexibility Analysis

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 Act 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.

As part of implementing the security plan, TSA expects security to be integrated into actions the same way safety has become integral to how things are done rather than adding layers or extra program costs. For this reason, in years beyond the initial year, costs are limited to an annual report, insuring their own plan is followed, and vetting any new employees. TSA has conducted an initial regulatory flexibility analysis. There are a substantial number of IACs and all-cargo carriers that are impacted, but TSA's initial finding is that the impacts are not substantial.

TSA has made several conservative assumptions in this analysis, which may have resulted in an overestimate of the costs of the proposed rule. For example, even though TSA believes most airports and all-cargo carriers have many elements of this rule already in place as good business practice or out of their own concerns for security, costing was done as if the entire group would be implementing these as new requirements. Based on information gathered through other efforts with the airports, TSA believes the airports have reached out to the aviation community and already successfully completed fingerprint-based criminal history records checks, and provided access badges and the associated access training. As a conservative measure, TSA has assumed that there are additional expenses to provide IDs for a limited group of employees at 100 locations. Also, there is a distinct possibility that very few additional law enforcement officers would be required,

[27] Paraphrase from *Business-Times* article of Dec. 9, 2003. The same elements were reported in numerous news services at approximately the same time.

but TSA allowed for the full-time equivalent coverage for two shifts for 20 of the carrier locations. This equated to an average of 0.6 per carrier and $27 million over the 10 years.

IACS

IACs are a subset of freight forwarders. The larger category of freight forwarders includes all modes of transportation.[29] Without better information, the characteristics of the total industry are assumed to apply to the IACs. The threshold for small business for this industry is $6 million and the distributions are as follows:

FREIGHT FORWARDING

[Number of firms in Duns for SIC 4731 02 by employees (not all records have employee data)]

Employees	Primary SIC	+Secondary SIC	# w FTE and sales data	Category %	Cmltv %
1–4	4154	4404	4311	55.2	55.23
5–9	1493	1602	1584	20.3	75.52
10–19	826	907	898	11.5	87.02
20–49	519	597	591	7.6	94.59
50+	336	427	422	5.4	100.00
Total	7328	7937	7806	100.0	

[Number of firms in Duns for SIC 4731 02 by sales]

Sales	Primary	+Secondary	Category %	Cmltv %
<$20k	5	5	0.0	0.0
$20–$50k	41	62	0.6	0.6
$50,001–$100k	109	167	1.6	2.2
$100,001–$249,999	749	880	8.3	10.5
$250k–$499,999	1763	1877	17.7	28.3
$500k–$999,999	3230	3360	31.8	60.0
$1m–$6m	3264	3503	33.1	93.1
>$6 million	627	725	6.9	100.0
Total	9788	10579	100.0	

Using the data above and the 3,800 population values in the analysis, all but 6.9% (or 3540) would be small entities for this analysis. To evaluate the impact, the data was segmented and the smallest of the small were examined to see if there was a significant impact. If the smallest group can be shown not to have significant impact, and because the relationship remains somewhat proportional as firm size increases, it is a reasonable conclusion that the overall impact is also insignificant. Once again, specific D&B firm data for the smallest 10.5% with revenues less than $250,000 was examined. This group provided 1110 useable records.

To estimate the impact, the individual cost items from the report above per employee are multiplied times the number of employees and then the cost per firm is added. The results are summed over the entire population which results in an impact of $72,700 on $170,278,465 of revenue or at a rate of .04% in the first or most expensive year. This rate of impact is not significant. See the following table for a summary of the calculation.

Item	Rate	Firm costs	Per employee costs
Annual Reporting	75/report/firm	75	
Training	4 hrs/employee @ $25		100
Security duties	20 Hrs/Firm @ 43	860	
Decertification	1 5 of Firms @250=2.50/Firm	2.5	
STA	55/Employee		55
Total		937.5	155

All-Cargo Operations

For All-Cargo Operations, DOT form 41 data from BTS TRASTATS was analyzed. The following distribution was found.

FREIGHT

[Aircraft size percentage]

Firm size	>=100	<100	Total
Large	77.7	0.8	78.5
Small	21.1	0.3	21.5

FREIGHT—Continued

[Aircraft size percentage]

Firm size	>=100	<100	Total
All Firms	98.8	1.2	100.0

[29] For a technical explanation of how the detailed data was segmented see the separate Regulatory Evaluation.

DEPARTURES

[Aircraft size percentage]

Firm size	>=100	<100	Total
Large	47.2	15.9	63.1
Small	22.9	14.0	36.9
All Firms	70.0	30.0	100.0

PASSENGER FLIGHT REPORTING FREIGHT

[Aircraft size percentage]

Firm size	Large	Small	Grand total
Large	88.3	8.5	96.7
Small	1.5	1.8	3.3
	89.8	10.2	100.0

Although it reflects revenue data for the large carriers (>$6 million) and many midsize carriers, too many small carriers are missing revenue data to make a cost comparison. TSA invites public comment on existing cost and revenue relationship as firms are experiencing under the existing security directives.

X. 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 proposed rule and has determined that it imposes the same costs on domestic and international entities and thus has a neutral trade impact.

XI. 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 proposed rule does not contain such a mandate. The requirements of Title II do not apply.

XII. 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 the Office of Management and Budget (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 proposes to amend current transportation security regulations to further enhance and improve the security of air cargo transportation. Specifically, TSA proposes to create a mandatory security program for all-cargo aircraft operations over 45,500 kg (100,309.3 lbs) and to amend existing security regulations and programs for aircraft operators, foreign air carriers, airport operators, and IACs. TSA is also proposing to expand security threat assessment requirements to new populations, including certain individuals who have unescorted access to air cargo and each officer, director and person who holds 25 percent or more of total outstanding voting stock of an Indirect Air Carrier or entity applying to become an IAC.

Use of: Security programs that are developed or amended as a result of this proposal 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. Security threat assessments conducted as a result of this proposal will be used to determine employment suitability for those who have unescorted access to cargo and each officer, director and person who holds 25 percent or more of total outstanding voting stock of an Indirect Air Carrier or entity applying to become an IAC.

Respondents (including number of): The likely respondents to this proposed information requirement are aircraft operators, foreign air carriers, IACs, and their employees who undergo security threat assessments for a total of approximately 37,090 respondents the first year and approximately 8,800 respondents each following year, for an average of 18,230 respondents for each of the next 3 years. The annual respondents include both new entrants and renewals. The number consists of 65 all-cargo operators, 3800 IACs, and their affected employees. TSA invites comments regarding these estimates.

Frequency: Upon implementation, security programs related to this proposal, including employee training records, will need to be kept on file and updated as necessary. Security threat assessments 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.

Annual Burden Estimate: The annual burden associated with the security program is estimated to be 30,920 hours, while the annual burden associated with the security threat assessments is estimated to average 3,559 hours over the next 3 years, for a combined average annual total of 34,479 hours.

The agency is inviting 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.

Individuals and organizations may submit comments on the information collection requirement by January 10, 2005, and should direct them via fax to the Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: DHS–TSA Desk Officer, at (202) 395–5806. Comments to OMB are most useful if received within 30 days of publication.

As protection provided by the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. The OMB control number for this information collection will be published in the **Federal Register** after OMB approves it.

XIII. International Compatibility

In keeping with U.S. 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 proposed regulations are consistent with ICAO Standards and Recommended Practices.

XIV. Executive Order 13132, Federalism

TSA has analyzed this proposed 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.

XV. 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.

Energy Impact

The energy impact of this document has been assessed in accordance with the Energy Policy and Conservation Act (EPCA) Public Law 94–163, as amended (42 U.S.C. 6362). We have determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects

49 CFR Part 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.

IX. The Proposed Amendment

For the reasons set forth above, the Transportation Security Administration proposes to amend Title 49 of the Code of Federal Regulations parts 1540, 1542, 1544, 1546, and 1548 as follows:

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

1. 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.

2. Amend § 1540.5 by revising the definition of ''indirect air carrier'' to read as follows:

§ 1540.5 Terms used in this subchapter.

* * * * *

Indirect air carrier 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.

* * * * *

3. Add Subpart C—Security Threat Assessments to read as follows:

Subpart C—Security Threat Assessments

Sec.

§ 1540.201 Applicability and definitions.

(a) This subpart applies to:

(1) Each aircraft operator operating under a full program described in 49 CFR 1544.101(a);

(2) Each foreign air carrier operating under a program described in 49 CFR 1546.101;

(3) Each indirect air carrier subject to 49 CFR part 1548; and

(4) Each individual with unescorted access to cargo under one of these programs.

(b) For purposes of this subpart, aircraft operator, foreign air carrier, and indirect air carrier listed in paragraphs (a)(1) through (a)(3) of this section are referred to as ''operator,'' and the individuals listed in paragraph (a)(4) of this section are referred to as ''individual.''

(c) An individual poses a security threat under this subpart when TSA determines that he or she is 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 an individual with unescorted access to cargo must complete 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 photo ID; 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.

(ii) Current mailing address, including residential address if different than current mailing address, and all other residential addresses for the previous seven years and email, if applicable.

(iii) Date and place of birth.

(iv) Social security number, if applicable.

(v) Citizenship status and date of naturalization if the individual is a naturalized citizen of the United States.

(vi) Alien registration number, if applicable.

(vii) 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. Your Social Security Number (SSN) or alien registration number will be used as your identification number in this process and to verify your identity. Furnishing this information, including your SSN or alien registration

number, is voluntary; however, failure to provide it will prevent the completion of your Security Threat Assessment, without which you may not be granted authorization to have unescorted access to cargo. *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.

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 completing 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 known or suspected security threat or that confirm an individual's identity.

(b) *Security Authorization for Unescorted Cargo Access.* TSA serves a Security Authorization on the individual and the operator if TSA determines that an individual does not pose a known or suspected security threat.

(c) *Initial Denial of Authorization for Unescorted Cargo Access.* TSA serves an Initial Denial of Authorization on the individual and the operator if TSA determines that the individual poses a known or suspected security threat. The Initial Denial of Authorization for Unescorted Cargo Access 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 Denial of Authorization, or does not request an extension of time within 30 days of the Initial Denial of Authorization in order to file an appeal, the Initial Denial of Authorization becomes a Final Denial of Authorization for Unescorted Cargo Access.

(d) *Final Denial of Authorization for Unescorted Cargo Access.* If TSA determines that an individual poses a known or suspected security threat, TSA serves a Final Denial of Authorization for Unescorted Cargo Access on the operator and the individual who appealed the Initial Denial of Authorization.

(e) *Withdrawal by TSA.* TSA serves a Withdrawal of the Initial Denial of Authorization for Unescorted Cargo Access on the individual and a Security Authorization for Unescorted Cargo Access on the operator, if the appeal results in a determination that the individual does not pose a threat to security.

(f) *Final Disposition.* Within 30 days of receipt of a Security Authorization for Unescorted Cargo Access or a Final Denial of Authorization for Unescorted Cargo Access, the operator must:

(1) Update the individual's permanent record to reflect the results of the Security Threat Assessment;

(2) Grant or deny the individual's unescorted access to cargo based on the results of the threat assessment.

§ 1540.207 Appeal procedures.

(a) *Scope.* This section applies to individuals who wish to appeal an Initial Denial of Authorization for Unescorted Cargo Access that is based on TSA's Security Threat Assessment.

(b) *Grounds for Appeal.* An individual may appeal an Initial Denial of Authorization for Unescorted Cargo Access if the individual is asserting that he or she does not pose a known or suspected security threat.

(c) *Appeal.* An individual initiates an appeal by submitting a written reply or written request for materials from TSA. If the individual fails to initiate an appeal within 30 days of receipt, the Initial Denial of Authorization for Unescorted Cargo Access becomes final, and TSA serves a Final Denial of Authorization for Unescorted Cargo Access on the operator and the individual.

(1) *Request for materials.* Within 30 days of the date of service of the Initial Denial of Authorization for Unescorted Cargo Access, the individual may serve upon TSA a written request for copies of the materials upon which the Initial Denial of Authorization 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 Denial of Authorization was based. TSA will not include any classified information or other protected information described in paragraph (f) of this section.

(3) *Correction of records.* If the Initial Denial of Authorization for Unescorted Cargo Access 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 Denial of Authorization for Unescorted Cargo Access within 30 days of service of the Initial Denial of Authorization, 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 known or suspected security threat.

(5) *Final determination.* Within 30 days after TSA receives the individual's reply, TSA serves a Final Denial of Authorization for Unescorted Cargo Access or a Withdrawal of the Initial Denial of Authorization.

(d) *Final Denial of Authorization for Unescorted Cargo Access.* (1) If TSA determines that the individual poses a security threat, TSA serves a Final Denial of Authorization for Unescorted Cargo Access upon the individual and the operator. The Final Denial of Authorization includes—

(2) A statement that TSA has reviewed the Initial Denial of Authorization, 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 known or suspected security threat.

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

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

(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.* For purposes of judicial review, the Final Denial of Authorization for Unescorted Cargo Access constitutes a final TSA order in accordance with 49 U.S.C. 46110.

§ 1540.209 Security threat assessment fee.

(a) *Imposition of fees.* The fee of $39.00 is required for TSA to conduct a security threat assessment for a candidate who has unescorted access to cargo and who is subject to the requirements of Part 1540, Subpart C, and each officer, director and person who holds 25 percent or more of total outstanding voting stock of an Indirect Air Carrier or entity applying to become an IAC.

(b) *Remittance of fees.* (1) A candidate must remit the fee required under this subpart to TSA, in a form and manner acceptable to TSA, each time the candidate or 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 United States currency and drawn on a United States bank.

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

PART 1542—AIRPORT SECURITY

4. 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.

5. Amend § 1542.1 by adding paragraph (d) to read as follows:

§ 1542.1 Applicability of this part.

* * * * *

(d) Each airport 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 of this part.

6. Revise paragraphs 1542.205(a) and (b)(2) and add paragraph (c) to read as follows:

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

(a) Each airport operator required to have a security program under § 1542.103(a) must establish at least one SIDA, which must include the following areas:

(1) Each secured area must be a SIDA.

(2) Each area that is regularly used to sort cargo that may be carried by an aircraft operator under a full or 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), and each area that is regularly used to load cargo on or unload cargo from such aircraft, must be a SIDA.

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

(b) * * *

(1) * * *

(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

7. 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.

8. Amend § 1544.101 by revising paragraphs (d)(1), (d)(4), and (e)(1) and add 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 more than 12,500 pounds.

* * * * *

(4) Is not under a full program, partial program, or 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 for all-cargo operations, §§ 1544.202, 1544.205(a), (b), and (d).

* * * * *

(h) *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) *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.

9. Add new § 1544.202 to read as follows:

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

Each aircraft operator operating under an 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, and for their property, to prevent or deter the carriage of unauthorized weapons, explosives, incendiaries, persons, and other destructive substances or items.

10. Amend § 1544.205 by revising paragraphs (a), (b), (c) introductory text, (c)(2) and (d); and adding new paragraphs (e) and (f) 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, an 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 unauthorized persons,

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 an all-cargo program, or a twelve-five program in an all-cargo operation, must ensure that cargo is screened and inspected for unauthorized persons, explosives, incendiaries, and other destructive substances or items 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 an 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) * * *

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

(d) *Refusal to transport.* Each aircraft operator operating under a full program, an all-cargo program, or a twelve-five program when 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 an 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, except as provided in its security program.

(f) *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.

11. Amend § 1544.225 by adding new paragraph (d):

§ 1544.225 Security of aircraft and facilities.

* * * * *

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

12. Add new § 1544.228 to read as follows:

§ 1544.228 Security threat assessments for cargo personnel.

This section applies to each aircraft operator operating under a full program or an all-cargo program, and to each individual who has unescorted access to cargo accepted by such an aircraft operator.

(a) Before gaining unescorted access to cargo, each individual 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 such a check under those sections; or

(2) A Security Threat Assessment under part 1540 subpart C of this chapter; or

(3) Another Security Threat Assessment approved by TSA.

(b) Each aircraft operator must ensure that each individual who has access to its cargo has either successfully completed one of the checks in paragraph (a) of this section or is escorted by such an individual.

13. Amend § 1544.229 by adding introductory text, revising paragraphs (a)(1)(iii) introductory text and (a)(1)(iii)(B) and adding new paragraph (a)(1)(iii)(C) 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 an 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) * * *

(B) Serving as an immediate supervisor (checkpoint security supervisor (CSS)), and the next supervisory level (shift or site supervisor), to those individuals described in paragraph (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 required to screen cargo under this part.

* * * * *

14. Add new § 1544.239 as follows:

§ 1544.239 Known shipper program.

This section applies to each aircraft operator operating under a full program under § 1544.101(a).

(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 its security program;

(2) Provide that the aircraft operator will separate known shipper shipments from unknown shipper shipments; 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 an applicant to the known shipper program; and

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

PART 1546—FOREIGN AIR CARRIER SECURITY

15. 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.

16. Amend § 1546.101 by revising the introductory text and paragraph (a) and by adding paragraphs (e) and (f):

§ 1546.101 Adoption and implementation.

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

(a) Section 1546.103(b) and subparts C, D, and E of this part for each operation with an airplane 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), 1546.213, and 1546.215 for each all-cargo operation with an airplane having a maximum certificated take-off weight more than 45,500 kg (100,309.3 pounds); and

(f) Sections 1546.103(b)(2) and (b)(4), 1546.202, 1546.205(a), (b) and (c), 1546.213, and 1546.215 for each all-cargo operation with an airplane having a maximum certificated take-off weight more than 12,500 pounds but no more than 45,500 kg.

17. 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) as applicable, must be designed to:

* * * * *

18. Add § 1546.202 to read as follows:

§ 1546.202 Persons and property on board the airplane.

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 airplane, and for their property, to prevent or deter the carriage of unauthorized weapons, explosives, incendiaries, persons, and other destructive substances or items.

19. Amend § 1546.205 by revising paragraphs (a) and (b) and adding new paragraphs (c), (d), (e) and (f) 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 unauthorized persons, explosives, incendiaries, and other destructive substances or items in cargo onboard an airplane.

(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 § 1546.101(a), (b), or (e) must use the procedure in its security program to control cargo that it accepts for transport on an airplane in a manner that:

(1) Prevents the carriage of any unauthorized persons, explosives, incendiaries, and other destructive substances or items aboard the airplane.

(2) Prevents access by unauthorized persons other than a foreign air carrier employee or its 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 explosives, incendiaries, unauthorized persons, and other destructive substances or items as provided in the foreign air carrier's security program, in accordance with § 1546.207, and § 1546.213 if applicable, before loading it on its airplane in the United States.

(e) *Acceptance of cargo in the United States.* Each foreign air carrier operating a program under § 1546.101(a), (b), or (e) 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 outside the United States.* Each foreign air carrier subject to this section that accepts cargo to be loaded on its airplane outside the United States must carry out the requirements of its security program.

20. Add a new § 1546.213 to read as follows:

§ 1546.213 Security threat assessments for cargo personnel in the United States.

This section applies to each foreign air carrier operating under § 1546.101(a), (b), or (e), and to each individual who has unescorted access in the United States.

(a) Before gaining unescorted access to cargo, each individual 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 such a check under those sections; or

(2) A Security Threat Assessment under part 1540 subpart C of this chapter; or

(3) Another Security Threat Assessment approved by TSA.

(b) Each foreign air carrier must ensure that each individual who has access to its cargo has either successfully completed one of the checks in paragraph (a) of this section or is escorted by such an individual.

21. Add new § 1546.215 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 its security program;

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

(2) Upon learning of a change to the information specified in (b)(1) of this section, corrections and updates to the information.

PART 1548—INDIRECT AIR CARRIER SECURITY

22. 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.

23. 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 or perform cargo services for an aircraft operator operating under a full program or an 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.

(b) *General requirements.* (1) The security program must provide for the security of persons and property traveling in air transportation against acts of criminal violence and air piracy and the introduction of any unauthorized person, explosive, incendiary or other destructive substances or items 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, agent, contractor or subcontractor of the indirect air carrier;

(ii) While the cargo is stored, en route, or otherwise being handled by an employee, agent, contractor or subcontractor 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 assure that its employees, agents, contractors, and subcontractors comply with the requirements of 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, explosive, incendiary or other destructive substances or items 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 curriculum used to accomplish the training required under § 1548.11 of persons who accept, handle, transport, or deliver cargo for or on behalf of the indirect air carrier.

* * * * *

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

(ii) The names, addresses, and dates of birth of each officer, director, and each person who holds 25 percent or more of total outstanding voting stock of the entity.

(iii) A signed statement from each person listed in paragraph (a)(1)(ii) of this section stating whether he or she has been an 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 (a)(1)(ii) of this section.

(v) Addresses of all business locations.

(vi) Whether the business is a ''small business'' pursuant to section 3 of the Small Business Act (15 U.S.C. 632).

(vii) Statement acknowledging and ensuring that each employee 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) Statement acknowledging and ensuring that each individual will successfully complete a Security Threat Assessment under § 1548.15 before the individual has 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 Directives upon determining that:

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

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

(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 initial application. This notification must be submitted to the designated official for reapproval within 30 days from the date the change occurred. 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.* (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. 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.

(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 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 part, its security program, and any Security Directives; 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 submit a request to TSA to amend its security program as follows:

(1) The request for an amendment must be filed with the designated official at least 45 calendar days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the designated official.

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

(3) An amendment to 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.

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

(5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator 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.

(6) 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.

(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 petitions the Administrator 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 the Administrator for reconsideration. The Administrator disposes of the petition within 30 calendar days of receipt by either directing the designated official to withdraw or amend the 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 Administrator no later than 15 calendar days before the effective date of 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 security 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 that notifies the indirect air carrier, in writing, of the facts, charges, and applicable law, regulation, or order that forms the basis for the determination.

(2) *IAC 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 a withdrawal of approval is issued, 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 Administrator 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 to 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) *Administrator's review.* The designated official transmits the petition together with all pertinent information to the Administrator for reconsideration. The Administrator 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 Administrator is a final order under 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 the date of personal delivery; 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 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.

25. 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 on board an aircraft of any unauthorized person, explosive, incendiary, and other destructive substances or items 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 part 1544 or 1546 of this chapter.

26. Add 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 any individual to perform any security-related duties to meet the requirements of its security program unless that individual has received training as specified in its security program including their individual responsibilities in § 1540.105 of this chapter.

(b) Each indirect air carrier must ensure that individuals who accept, handle, transport, or deliver cargo for or on behalf of the indirect air carrier have knowledge of the applicable provisions of this part, applicable Security Directives and Information Circulars, the approved airport security program applicable to their location, and 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.

(c) Each indirect air carrier must ensure that each individual under paragraph (b) of this section for the indirect air carrier successfully completes recurrent training at least annually on their individual responsibilities in § 1540.105 of this chapter, the applicable provisions of this part, applicable Security Directives and Information Circulars, the approved airport security program applicable to their location, and 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.

27. Add new § 1548.13 to read as follows:

§ 1548.13 Security coordinators.

(a) *Indirect Air Carrier Security Coordinator.* 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.

(b) [Reserved].

28. Add new § 1548.15 to read as follows:

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

This section applies to each indirect air carrier, and to each individual who has unescorted access to cargo accepted by such an indirect air carrier.

(a) Before gaining unescorted access to cargo, each individual must successfully complete either—

(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 such a check under those sections; or

(2) A Security Threat Assessment under part 1540 of this chapter; or

(3) Another Security Threat Assessment approved by TSA.

(b) Each indirect air carrier must ensure that each individual who has access to its cargo has either successfully completed one of the checks in paragraph (a) of this section or is escorted by such an individual.

29. Add new § 1548.17 to read as follows:

§ 1548.17 Known shipper program.

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

(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 shipments from unknown shipper shipments.

(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 the known shipper program; and

(2) Upon learning of a change to the information specified in subparagraph (b)(1) of this paragraph, corrections and updates of this information.

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

(b) Each indirect air carrier required to have an approved indirect air carrier security program must comply with each Security Directive issued to the indirect air carrier by TSA, within the time prescribed in the Security Directive for compliance.

(c) Each indirect air carrier that receives a Security Directive must—

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

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

(d) In the event that the 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. The indirect air carrier must submit the proposed alternative measures within the time prescribed in the Security Directive. The indirect air carrier must implement any alternative measures approved by TSA.

(e) Each indirect air carrier that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to TSA. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive.

(f) Each 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:

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

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

Issued in Arlington, VA, on November 3, 2004.

David M. Stone,

Assistant Secretary.

[FR Doc. 04–24883 Filed 11–9–04; 8:45 am]

BILLING CODE 4910–62–P