

§ 1540.303

49 CFR Ch. XII (10–1–10 Edition)

§ 1540.303 [Reserved]

PART 1542—AIRPORT SECURITY

Subpart A—General

Sec.

- 1542.1 Applicability of this part.
- 1542.3 Airport security coordinator.
- 1542.5 Inspection authority.

Subpart B—Airport Security Program

- 1542.101 General requirements.
- 1542.103 Content.
- 1542.105 Approval and amendments.
- 1542.103 Changed conditions affecting security.
- 1542.109 Alternate means of compliance.
- 1542.111 Exclusive area agreements.
- 1542.113 Airport tenant security programs.

Subpart C—Operations

- 1542.201 Security of the secured area.
- 1542.203 Security of the air operations area (AOA).
- 1542.205 Security of the security identification display area (SIDA).
- 1542.207 Access control systems.
- 1542.209 Fingerprint-based criminal history records checks (CHRC).
- 1542.211 Identification systems.
- 1542.213 Training.
- 1542.215 Law enforcement support.
- 1542.217 Law enforcement personnel.
- 1542.219 Supplementing law enforcement personnel.
- 1542.221 Records of law enforcement response.

Subpart D—Contingency Measures

- 1542.301 Contingency plan.
- 1542.303 Security Directives and Information Circulars.
- 1542.305 Public advisories.
- 1542.307 Incident management.

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

SOURCE: 67 FR 8355, Feb. 22, 2002, unless otherwise noted.

Subpart A—General

§ 1542.1 Applicability of this part.

This part describes aviation security rules governing:

(a) The operation of airports regularly serving aircraft operations required to be under a security program under part 1544 of this chapter, as described in this part.

(b) The operation of airport regularly serving foreign air carrier operations required to be under a security program under part 1546 of this chapter, as described in this part.

(c) Each airport operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular issued by the Designated official for Civil Aviation Security.

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

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

§ 1542.3 Airport security coordinator.

(a) Each airport operator must designate one or more Airport Security Coordinator(s) (ASC) in its security program.

(b) The airport operator must ensure that one or more ASCs:

(1) Serve as the airport operator's primary and immediate contact for security-related activities and communications with TSA. Any individual designated as an ASC may perform other duties in addition to those described in this paragraph (b).

(2) Is available to TSA on a 24-hour basis.

(3) Review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with this part, its security program, and applicable Security Directives.

(4) Immediately initiate corrective action for any instance of non-compliance with this part, its security program, and applicable Security Directives.

(5) Review and control the results of employment history, verification, and criminal history records checks required under § 1542.209.

(6) Serve as the contact to receive notification from individuals applying for unescorted access of their intent to seek correction of their criminal history record with the FBI.

(c) After July 17, 2003, no airport operator may use, nor may it designate any person as, an ASC unless that individual has completed subject matter training, as specified in its security program, to prepare the individual to assume the duties of the position. The airport operator must maintain ASC training documentation until at least 180 days after the withdrawal of an individual's designation as an ASC.

(d) An individual's satisfactory completion of initial ASC training required under paragraph (c) of this section satisfies that requirement for all future ASC designations for that individual, except for site specific information, unless there has been a two or more year break in service as an active and designated ASC.

§ 1542.5 Inspection authority.

(a) Each airport operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with—

(1) This subchapter and any security program under this subchapter, and part 1520 of this chapter; and

(2) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of TSA, each airport operator must provide evidence of compliance with this part and its airport security program, including copies of records.

(c) TSA may enter and be present within secured areas, AOA's, and SIDA's without access media or identification media issued or approved by an airport operator or aircraft operator, in order to inspect or test compliance, or perform other such duties as TSA may direct.

(d) At the request of TSA and upon the completion of SIDA training as required in a security program, each airport operator promptly must issue to TSA personnel access and identification media to provide TSA personnel with unescorted access to, and movement within, secured areas, AOA's, and SIDA's.

(e) TSA may enter and be present at an airport that does not have a security program under this part, without

access media or identification media issued or approved by an airport operator or aircraft operator, to inspect an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

Subpart B—Airport Security Program

§ 1542.101 General requirements.

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

(1) Provides for the safety and security of persons and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft;

(2) Is in writing and is signed by the airport operator;

(3) Includes the applicable items listed in § 1542.103;

(4) Includes an index organized in the same subject area sequence as § 1542.103; and

(5) Has been approved by TSA.

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

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

(1) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know; and

(2) Refer all requests for SSI by other persons to TSA.

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

§ 1542.103 Content.

(a) *Complete program.* Except as otherwise approved by TSA, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(1) or

§ 1542.103

49 CFR Ch. XII (10–1–10 Edition)

§ 1546.101(a) of this chapter, must include in its security program the following:

(1) The name, means of contact, duties, and training requirements of the ASC required under § 1542.3.

(2) [Reserved]

(3) A description of the secured areas, including—

(i) A description and map detailing boundaries and pertinent features;

(ii) Each activity or entity on, or adjacent to, a secured area that affects security;

(iii) Measures used to perform the access control functions required under § 1542.201(b)(1);

(iv) Procedures to control movement within the secured area, including identification media required under § 1542.201(b)(3); and

(v) A description of the notification signs required under § 1542.201(b)(6).

(4) A description of the AOA, including—

(i) A description and map detailing boundaries, and pertinent features;

(ii) Each activity or entity on, or adjacent to, an AOA that affects security;

(iii) Measures used to perform the access control functions required under § 1542.203(b)(1);

(iv) Measures to control movement within the AOA, including identification media as appropriate; and

(v) A description of the notification signs required under § 1542.203(b)(4).

(5) A description of the SIDA's, including—

(i) A description and map detailing boundaries and pertinent features; and

(ii) Each activity or entity on, or adjacent to, a SIDA.

(6) A description of the sterile areas, including—

(i) A diagram with dimensions detailing boundaries and pertinent features;

(ii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and

(iii) Measures used to control access as specified in § 1542.207.

(7) Procedures used to comply with § 1542.209 regarding fingerprint-based criminal history records checks.

(8) A description of the personnel identification systems as described in § 1542.211.

(9) Escort procedures in accordance with § 1542.211(e).

(10) Challenge procedures in accordance with § 1542.211(d).

(11) Training programs required under §§ 1542.213 and 1542.217(c)(2), if applicable.

(12) A description of law enforcement support used to comply with § 1542.215(a).

(13) A system for maintaining the records described in § 1542.221.

(14) The procedures and a description of facilities and equipment used to support TSA inspection of individuals and property, and aircraft operator or foreign air carrier screening functions of parts 1544 and 1546 of this chapter.

(15) A contingency plan required under § 1542.301.

(16) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(17) Procedures for posting of public advisories as specified in § 1542.305.

(18) Incident management procedures used to comply with § 1542.307.

(19) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions.

(20) Each exclusive area agreement as specified in § 1542.111.

(21) Each airport tenant security program as specified in § 1542.113.

(b) *Supporting program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(2) or (f), or § 1546.101(b) or (c) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC, as required under § 1542.3.

(2) A description of the law enforcement support used to comply with § 1542.215(a).

(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 1542.221.

(5) The contingency plan required under § 1542.301.

(6) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(7) Procedures for public advisories as specified in § 1542.305.

(8) Incident management procedures used to comply with § 1542.307.

(c) *Partial program.* Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(b) or § 1546.101(d) of this chapter, must include in its security program a description of the following:

(1) Name, means of contact, duties, and training requirements of the ASC as required under § 1542.3.

(2) A description of the law enforcement support used to comply with § 1542.215(b).

(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 1542.221.

(5) Procedures for the distribution, storage, and disposal of security programs, Security Directives, Information Circulars, implementing instructions, and, as appropriate, classified information.

(6) Procedures for public advisories as specified in § 1542.305.

(7) Incident management procedures used to comply with § 1542.307.

(d) *Use of appendices.* The airport operator may comply with paragraphs (a), (b), and (c) of this section by including in its security program, as an appendix, any document that contains the information required by paragraphs (a), (b), and (c) of this section. The appendix must be referenced in the corresponding section(s) of the security program.

§ 1542.105 Approval and amendments.

(a) *Initial approval of security program.* Unless otherwise authorized by the designated official, each airport operator required to have a security program under this part must submit its initial proposed security program to the des-

ignated official for approval at least 90 days before the date any aircraft operator or foreign air carrier required to have a security program under part 1544 or part 1546 of this chapter is expected to begin operations. Such requests will be processed as follows:

(1) The designated official, within 30 days after receiving the proposed security program, will either approve the program or give the airport operator written notice to modify the program to comply with the applicable requirements of this part.

(2) The airport operator may either submit a modified security program to the designated official for approval, or petition the Administrator to reconsider the notice to modify within 30 days of receiving a notice to modify. A petition for reconsideration must be filed with the designated official.

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

(b) *Amendment requested by an airport operator.* Except as provided in § 1542.103(c), an airport operator may submit a request to the designated official to amend its security program, as follows:

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

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

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

§ 1542.107

49 CFR Ch. XII (10–1–10 Edition)

(4) Within 30 days after receiving a denial, the airport operator may petition the Administrator to reconsider the denial.

(5) Upon receipt of a petition for reconsideration, the designated official either approves the request to amend or transmits the petition within 30 days of receipt, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the designated official to approve the amendment or affirming the denial.

(c) *Amendment by TSA.* If safety and the public interest require an amendment, the designated official may amend a security program as follows:

(1) The designated official sends to the airport operator a notice, in writing, of the proposed amendment, fixing a period of not less than 30 days within which the airport operator may submit written information, views, and arguments on the amendment.

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

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

(d) *Emergency amendments.* Notwithstanding paragraph (c) of this section, if the designated official finds that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air

commerce that makes procedures in this section contrary to the public interest, the designated official may issue an amendment, effective without stay on the date the airport operator receives the notice of it. In such a case, the designated official must incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The airport operator may file a petition for reconsideration under paragraph (c) of this section; however, this does not stay the effective date of the emergency amendment.

§ 1542.107 Changed conditions affecting security.

(a) After approval of the security program, each airport operator must notify TSA when changes have occurred to the—

(1) Measures, training, area descriptions, or staffing, described in the security program;

(2) Operations of an aircraft operator or foreign air carrier that would require modifications to the security program as required under § 1542.103; or

(3) Layout or physical structure of any area under the control of the airport operator, airport tenant, aircraft operator, or foreign air carrier used to support the screening process, access, presence, or movement control functions required under part 1542, 1544, or 1546 of this chapter.

(b) Each airport operator must notify TSA no more than 6 hours after the discovery of any changed condition described in paragraph (a) of this section, or within the time specified in its security program, of the discovery of any changed condition described in paragraph (a) of this section. The airport operator must inform TSA of each interim measure being taken to maintain adequate security until an appropriate amendment to the security program is approved. Each interim measure must be acceptable to TSA.

(c) For changed conditions expected to be less than 60 days duration, each airport operator must forward the information required in paragraph (b) of this section in writing to TSA within 72 hours of the original notification of

the change condition(s). TSA will notify the airport operator of the disposition of the notification in writing. If approved by TSA, this written notification becomes a part of the airport security program for the duration of the changed condition(s).

(d) For changed conditions expected to be 60 days or more duration, each airport operator must forward the information required in paragraph (b) of this section in the form of a proposed amendment to the airport operator's security program, as required under § 1542.105. The request for an amendment must be made within 30 days of the discovery of the changed condition(s). TSA will respond to the request in accordance with § 1542.105.

§ 1542.109 Alternate means of compliance.

If in TSA's judgment, the overall safety and security of the airport, and aircraft operator or foreign air carrier operations are not diminished, TSA may approve a security program that provides for the use of alternate measures. Such a program may be considered only for an operator of an airport at which service by aircraft operators or foreign air carriers under part 1544 or 1546 of this chapter is determined by TSA to be seasonal or infrequent.

§ 1542.111 Exclusive area agreements.

(a) TSA may approve an amendment to an airport security program under which an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter assumes responsibility for specified security measures for all or portions of the secured area, AOA, or SIDA, including access points, as provided in § 1542.201, § 1542.203, or § 1542.205. The assumption of responsibility must be exclusive to one aircraft operator or foreign air carrier, and shared responsibility among aircraft operators or foreign air carriers is not permitted for an exclusive area.

(b) An exclusive area agreement must be in writing, signed by the airport operator and aircraft operator or foreign air carrier, and maintained in the airport security program. This agreement must contain the following:

(1) A description, a map, and, where appropriate, a diagram of the boundaries and pertinent features of each area, including individual access points, over which the aircraft operator or foreign air carrier will exercise exclusive security responsibility.

(2) A description of the measures used by the aircraft operator or foreign air carrier to comply with § 1542.201, § 1542.203, or § 1542.205, as appropriate.

(3) Procedures by which the aircraft operator or foreign air carrier will immediately notify the airport operator and provide for alternative security measures when there are changed conditions as described in § 1542.103(a).

(c) Any exclusive area agreements in effect on November 14, 2001, must meet the requirements of this section and § 1544.227 no later than November 14, 2002.

§ 1542.113 Airport tenant security programs.

(a) TSA may approve an airport tenant security program as follows:

(1) The tenant must assume responsibility for specified security measures of the secured area, AOA, or SIDA as provided in §§ 1542.201, 1542.203, and 1542.205.

(2) The tenant may not assume responsibility for law enforcement support under § 1542.215.

(3) The tenant must assume the responsibility within the tenant's leased areas or areas designated for the tenant's exclusive use. A tenant may not assume responsibility under a tenant security program for the airport passenger terminal.

(4) Responsibility must be exclusive to one tenant, and shared responsibility among tenants is not permitted.

(5) TSA must find that the tenant is able and willing to carry out the airport tenant security program.

(b) An airport tenant security program must be in writing, signed by the airport operator and the airport tenant, and maintained in the airport security program. The airport tenant security program must include the following:

(1) A description and a map of the boundaries and pertinent features of

§ 1542.201

49 CFR Ch. XII (10–1–10 Edition)

each area over which the airport tenant will exercise security responsibilities.

(2) A description of the measures the airport tenant has assumed.

(3) Measures by which the airport operator will monitor and audit the tenant's compliance with the security program.

(4) Monetary and other penalties to which the tenant may be subject if it fails to carry out the airport tenant security program.

(5) Circumstances under which the airport operator will terminate the airport tenant security program for cause.

(6) A provision acknowledging that the tenant is subject to inspection by TSA in accordance with §1542.5.

(7) A provision acknowledging that individuals who carry out the tenant security program are contracted to or acting for the airport operator and are required to protect sensitive information in accordance with part 1520 of this chapter, and may be subject to civil penalties for failing to protect sensitive security information.

(8) Procedures by which the tenant will immediately notify the airport operator of and provide for alternative security measures for changed conditions as described in §1542.103(a).

(c) If TSA has approved an airport tenant security program, the airport operator may not be found to be in violation of a requirement of this part in any case in which the airport operator demonstrates that:

(1) The tenant or an employee, permittee, or invitee of the tenant, is responsible for such violation; and

(2) The airport operator has complied with all measures in its security program to ensure the tenant has complied with the airport tenant security program.

(d) TSA may amend or terminate an airport tenant security program in accordance with §1542.105.

Subpart C—Operations

§ 1542.201 Security of the secured area.

(a) Each airport operator required to have a security program under §1542.103(a) must establish at least one secured area.

(b) Each airport operator required to establish a secured area must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured area by doing the following:

(1) Establish and carry out measures for controlling entry to secured areas of the airport in accordance with §1542.207.

(2) Provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the secured area by an individual whose access is not authorized in accordance with its security program.

(3) Establish and carry out a personnel identification system described under §1542.211.

(4) Subject each individual to employment history verification as described in §1542.209 before authorizing unescorted access to a secured area.

(5) Train each individual before granting unescorted access to the secured area, as required in §1542.213(b).

(6) Post signs at secured area access points and on the perimeter that provide warning of the prohibition against unauthorized entry. Signs must be posted by each airport operator in accordance with its security program not later than November 14, 2003.

§ 1542.203 Security of the air operations area (AOA).

(a) Each airport operator required to have a security program under §1542.103(a) must establish an AOA, unless the entire area is designated as a secured area.

(b) Each airport operator required to establish an AOA must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA by doing the following:

(1) Establish and carry out measures for controlling entry to the AOA of the airport in accordance with §1542.207.

(2) Provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the AOA by an individual whose access is not authorized in accordance with its security program.

(3) Provide security information as described in §1542.213(c) to each individual with unescorted access to the AOA.

(4) Post signs on AOA access points and perimeters that provide warning of the prohibition against unauthorized entry to the AOA. Signs must be posted by each airport operator in accordance with its security program not later than November 14, 2003.

(5) If approved by TSA, the airport operator may designate all or portions of its AOA as a SIDA, or may use another personnel identification system, as part of its means of meeting the requirements of this section. If it uses another personnel identification system, the media must be clearly distinguishable from those used in the secured area and SIDA.

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

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

(1) Each secured area must be a SIDA.

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

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

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

(b) Each airport operator required to establish a SIDA must establish and

carry out measures to prevent the unauthorized presence and movement of individuals in the SIDA and must do the following:

(1) Establish and carry out a personnel identification system described under §1542.211.

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

(3) Train each individual before granting unescorted access to the SIDA, as required in §1542.213(b).

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

[67 FR 8355, Feb. 22, 2002, as amended at 71 FR 30509, May 26, 2006]

§ 1542.207 Access control systems.

(a) *Secured area.* Except as provided in paragraph (b) of this section, the measures for controlling entry to the secured area required under §1542.201(b)(1) must—

(1) Ensure that only those individuals authorized to have unescorted access to the secured area are able to gain entry;

(2) Ensure that an individual is immediately denied entry to a secured area when that person's access authority for that area is withdrawn; and

(3) Provide a means to differentiate between individuals authorized to have access to an entire secured area and individuals authorized access to only a particular portion of a secured area.

(b) *Alternative systems.* TSA may approve an amendment to a security program that provides alternative measures that provide an overall level of security equal to that which would be provided by the measures described in paragraph (a) of this section.

(c) *Air operations area.* The measures for controlling entry to the AOA required under §1542.203(b)(1) must incorporate accountability procedures to maintain their integrity.

(d) *Secondary access media.* An airport operator may issue a second access medium to an individual who has unescorted access to secured areas or the AOA, but is temporarily not in possession of the original access medium,

§ 1542.209

49 CFR Ch. XII (10–1–10 Edition)

if the airport operator follows measures and procedures in the security program that—

- (1) Verifies the authorization of the individual to have unescorted access to secured areas or AOAs;
- (2) Restricts the time period of entry with the second access medium;
- (3) Retrieves the second access medium when expired;
- (4) Deactivates or invalidates the original access medium until the individual returns the second access medium; and
- (5) Provides that any second access media that is also used as identification media meet the criteria of § 1542.211(b).

§ 1542.209 Fingerprint-based criminal history records checks (CHRC).

(a) *Scope.* The following persons are within the scope of this section—

- (1) Each airport operator and airport user.
- (2) Each individual currently having unescorted access to a SIDA, and each individual with authority to authorize others to have unescorted access to a SIDA (referred to as unescorted access authority).
- (3) Each individual seeking unescorted access authority.
- (4) Each airport user and aircraft operator making a certification to an airport operator pursuant to paragraph (n) of this section, or 14 CFR 108.31(n) in effect prior to November 14, 2001 (see 14 CFR Parts 60 to 139 revised as of January 1, 2001). An airport user, for the purposes of this section only, is any person other than an aircraft operator subject to § 1544.229 of this chapter making a certification under this section.

(b) *Individuals seeking unescorted access authority.* Except as provided in paragraph (m) of this section, each airport operator must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based CHRC that does not disclose that he or she has a disqualifying criminal offense, as described in paragraph (d) of this section.

(c) *Individuals who have not had a CHRC.* (1) Except as provided in paragraph (m) of this section, each airport operator must ensure that after De-

cember 6, 2002, no individual retains unescorted access authority, unless the airport operator has obtained and submitted a fingerprint under this part.

(2) When a CHRC discloses a disqualifying criminal offense for which the conviction or finding of not guilty by reason of insanity was on or after December 6, 1991, the airport operator must immediately suspend that individual's authority.

(d) *Disqualifying criminal offenses.* An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the disqualifying crimes listed in this paragraph (d) in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority. The disqualifying criminal offenses are as follows—

- (1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.
- (2) Interference with air navigation; 49 U.S.C. 46308.
- (3) Improper transportation of a hazardous material; 49 U.S.C. 46312.
- (4) Aircraft piracy; 49 U.S.C. 46502.
- (5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504.
- (6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.
- (7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.
- (8) Conveying false information and threats; 49 U.S.C. 46507.
- (9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).
- (10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.
- (11) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.
- (12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.
- (13) Murder.
- (14) Assault with intent to murder.
- (15) Espionage.
- (16) Sedition.
- (17) Kidnapping or hostage taking.

- (18) Treason.
 - (19) Rape or aggravated sexual abuse.
 - (20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
 - (21) Extortion.
 - (22) Armed or felony unarmed robbery.
 - (23) Distribution of, or intent to distribute, a controlled substance.
 - (24) Felony arson.
 - (25) Felony involving a threat.
 - (26) Felony involving—
 - (i) Willful destruction of property;
 - (ii) Importation or manufacture of a controlled substance;
 - (iii) Burglary;
 - (iv) Theft;
 - (v) Dishonesty, fraud, or misrepresentation;
 - (vi) Possession or distribution of stolen property;
 - (vii) Aggravated assault;
 - (viii) Bribery; or
 - (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.
 - (27) Violence at international airports; 18 U.S.C. 37.
 - (28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d).
- (e) *Fingerprint application and processing.* (1) At the time of fingerprinting, the airport operator must provide the individual to be fingerprinted a fingerprint application that includes only the following—
- (i) The disqualifying criminal offenses described in paragraph (d) of this section.
 - (ii) A statement that the individual signing the application does not have a disqualifying criminal offense.
 - (iii) A statement informing the individual that Federal regulations under 49 CFR 1542.209 (l) impose a continuing obligation to disclose to the airport operator within 24 hours if he or she is convicted of any disqualifying criminal offense that occurs while he or she has unescorted access authority. After February 17, 2002, the airport operator may use statements that have already been printed referring to 14 CFR 107.209 until stocks of such statements are used up.
 - (iv) A statement reading, “The information I have provided on this applica-

tion is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or both. (See section 1001 of Title 18 United States Code.)”

(v) A line for the printed name of the individual.

(vi) A line for the individual’s signature and date of signature.

(2) Each individual must complete and sign the application prior to submitting his or her fingerprints.

(3) The airport operator must verify the identity of the individual through two forms of identification prior to fingerprinting, and ensure that the printed name on the fingerprint application is legible. At least one of the two forms of identification must have been issued by a government authority, and at least one must include a photo.

(4) The airport operator must advise the individual that:

(i) A copy of the criminal record received from the FBI will be provided to the individual, if requested by the individual in writing; and

(ii) The ASC is the individual’s point of contact if he or she has questions about the results of the CHRC.

(5) The airport operator must collect, control, and process one set of legible and classifiable fingerprints under direct observation of the airport operator or a law enforcement officer.

(6) Fingerprints may be obtained and processed electronically, or recorded on fingerprint cards approved by the FBI and distributed by TSA for that purpose.

(7) The fingerprint submission must be forwarded to TSA in the manner specified by TSA.

(f) *Fingerprinting fees.* Airport operators must pay for all fingerprints in a form and manner approved by TSA. The payment must be made at the designated rate (available from the local TSA security office) for each set of fingerprints submitted. Information about payment options is available through the designated TSA headquarters point of contact. Individual personal checks are not acceptable.

(g) *Determination of arrest status.* (1) When a CHRC on an individual seeking

unescorted access authority discloses an arrest for any disqualifying criminal offense listed in paragraph (d) of this section without indicating a disposition, the airport operator must determine, after investigation, that the arrest did not result in a disqualifying offense before granting that authority. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(2) When a CHRC on an individual with unescorted access authority discloses an arrest for any disqualifying criminal offense without indicating a disposition, the airport operator must suspend the individual's unescorted access authority not later than 45 days after obtaining the CHRC unless the airport operator determines, after investigation, that the arrest did not result in a disqualifying criminal offense. If there is no disposition, or if the disposition did not result in a conviction or in a finding of not guilty by reason of insanity of one of the offenses listed in paragraph (d) of this section, the individual is not disqualified under this section.

(3) The airport operator may only make the determinations required in paragraphs (g)(1) and (g)(2) of this section for individuals for whom it is issuing, or has issued, unescorted access authority, and who are not covered by a certification from an aircraft operator under paragraph (n) of this section. The airport operator may not make determinations for individuals described in § 1544.229 of this chapter.

(h) *Correction of FBI records and notification of disqualification.* (1) Before making a final decision to deny unescorted access authority to an individual described in paragraph (b) of this section, the airport operator must advise him or her that the FBI criminal record discloses information that would disqualify him or her from receiving or retaining unescorted access authority and provide the individual with a copy of the FBI record if he or she requests it.

(2) The airport operator must notify an individual that a final decision has

been made to grant or deny unescorted access authority.

(3) Immediately following the suspension of unescorted access authority of an individual, the airport operator must advise him or her that the FBI criminal record discloses information that disqualifies him or her from retaining unescorted access authority and provide the individual with a copy of the FBI record if he or she requests it.

(i) *Corrective action by the individual.* The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record, subject to the following conditions—

(1) For an individual seeking unescorted access authority on or after December 6, 2001, the following applies:

(i) Within 30 days after being advised that the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the airport operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The airport operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to granting unescorted access authority.

(ii) If no notification, as described in paragraph (h)(1) of this section, is received within 30 days, the airport operator may make a final determination to deny unescorted access authority.

(2) For an individual with unescorted access authority before December 6, 2001, the following applies: Within 30 days after being advised of suspension because the criminal record received from the FBI discloses a disqualifying criminal offense, the individual must notify the airport operator in writing of his or her intent to correct any information he or she believes to be inaccurate. The airport operator must obtain a copy, or accept a copy from the individual, of the revised FBI record, or a certified true copy of the information from the appropriate court, prior to reinstating unescorted access authority.

(j) *Limits on dissemination of results.* Criminal record information provided by the FBI may be used only to carry

out this section and §1544.229 of this chapter. No person may disseminate the results of a CHRC to anyone other than:

(1) The individual to whom the record pertains, or that individual's authorized representative.

(2) Officials of other airport operators who are determining whether to grant unescorted access to the individual under this part.

(3) Aircraft operators who are determining whether to grant unescorted access to the individual or authorize the individual to perform screening functions under part 1544 of this chapter.

(4) Others designated by TSA.

(k) *Recordkeeping.* The airport operator must maintain the following information:

(1) *Investigations conducted before December 6, 2001.* The airport operator must maintain and control the access or employment history investigation files, including the criminal history records results portion, or the appropriate certifications, for investigations conducted before December 6, 2001.

(2) *Fingerprint application process on or after December 6, 2001.* Except when the airport operator has received a certification under paragraph (n) of this section, the airport operator must physically maintain, control, and, as appropriate, destroy the fingerprint application and the criminal record. Only direct airport operator employees may carry out the responsibility for maintaining, controlling, and destroying criminal records.

(3) *Certification on or after December 6, 2001.* The airport operator must maintain the certifications provided under paragraph (n) of this section.

(4) *Protection of records—all investigations.* The records required by this section must be maintained in a manner that is acceptable to TSA and in a manner that protects the confidentiality of the individual.

(5) *Duration—all investigations.* The records identified in this section with regard to an individual must be maintained until 180 days after the termination of the individual's unescorted access authority. When files are no longer maintained, the criminal record must be destroyed.

(l) *Continuing responsibilities.* (1) Each individual with unescorted access authority on December 6, 2001, who had a disqualifying criminal offense in paragraph (d) of this section on or after December 6, 1991, must, by January 7, 2002, report the conviction to the airport operator and surrender the SIDA access medium to the issuer.

(2) Each individual with unescorted access authority who has a disqualifying criminal offense must report the offense to the airport operator and surrender the SIDA access medium to the issuer within 24 hours of the conviction or the finding of not guilty by reason of insanity.

(3) If information becomes available to the airport operator or the airport user indicating that an individual with unescorted access authority has a disqualifying criminal offense, the airport operator must determine the status of the conviction. If a disqualifying offense is confirmed the airport operator must immediately revoke any unescorted access authority.

(m) *Exceptions.* Notwithstanding the requirements of this section, an airport operator must authorize the following individuals to have unescorted access authority:

(1) An employee of the Federal, state, or local government (including a law enforcement officer) who, as a condition of employment, has been subjected to an employment investigation that includes a criminal records check.

(2) Notwithstanding the requirements of this section, an airport operator may authorize the following individuals to have unescorted access authority:

(i) An individual who has been continuously employed in a position requiring unescorted access authority by another airport operator, airport user, or aircraft operator, or contractor to such an entity, provided the grant for his or her unescorted access authority was based upon a fingerprint-based CHRC through TSA or FAA.

(ii) An individual who has been continuously employed by an aircraft operator or aircraft operator contractor, in a position with authority to perform screening functions, provided the grant for his or her authority to perform screening functions was based upon a

§ 1542.211

fingerprint-based CHRC through TSA or FAA.

(n) *Certifications by aircraft operators.* An airport operator is in compliance with its obligation under paragraph (b) or (c) of this section when the airport operator accepts, for each individual seeking unescorted access authority, certification from an aircraft operator subject to part 1544 of this chapter indicating it has complied with §1544.229 of this chapter for the aircraft operator's employees and contractors seeking unescorted access authority. If the airport operator accepts a certification from the aircraft operator, the airport operator may not require the aircraft operator to provide a copy of the CHRC.

(o) *Airport operator responsibility.* The airport operator must—

(1) Designate the ASC, in the security program, or a direct employee if the ASC is not a direct employee, to be responsible for maintaining, controlling, and destroying the criminal record files when their maintenance is no longer required by paragraph (k) of this section.

(2) Designate the ASC, in the security program, to serve as the contact to receive notification from individuals applying for unescorted access authority of their intent to seek correction of their FBI criminal record.

(3) Audit the employment history investigations performed by the airport operator in accordance with this section and 14 CFR 107.31 in effect prior to November 14, 2001 (see 14 CFR Parts 60 through 139 revised as of January 1, 2001), and those investigations conducted by the airport users who provided certification to the airport operator. The audit program must be set forth in the airport security program.

(p) *Airport user responsibility.* (1) The airport user must report to the airport operator information, as it becomes available, that indicates an individual with unescorted access authority may have a disqualifying criminal offense.

(2) The airport user must maintain and control, in compliance with paragraph (k) of this section, the employment history investigation files for investigations conducted before December 6, 2001, unless the airport operator

49 CFR Ch. XII (10-1-10 Edition)

decides to maintain and control the employment history investigation file.

(3) The airport user must provide the airport operator with either the name or title of the individual acting as custodian of the files described in this paragraph (p), the address of the location where the files are maintained, and the phone number of that location. The airport user must provide the airport operator and TSA with access to these files.

§ 1542.211 Identification systems.

(a) *Personnel identification system.* The personnel identification system under §§ 1542.201(b)(3) and 1542.205(b)(1) must include the following:

(1) Personnel identification media that—

(i) Convey a full-face image, full name, employer, and identification number of the individual to whom the identification medium is issued;

(ii) Indicate clearly the scope of the individual's access and movement privileges;

(iii) Indicate clearly an expiration date; and

(iv) Are of sufficient size and appearance as to be readily observable for challenge purposes.

(2) Procedures to ensure that each individual in the secured area or SIDA continuously displays the identification medium issued to that individual on the outermost garment above waist level, or is under escort.

(3) Procedures to ensure accountability through the following:

(i) Retrieving expired identification media and media of persons who no longer have unescorted access authority.

(ii) Reporting lost or stolen identification media.

(iii) Securing unissued identification media stock and supplies.

(iv) Auditing the system at a minimum of once a year or sooner, as necessary, to ensure the integrity and accountability of all identification media.

(v) As specified in the security program, revalidate the identification system or reissue identification media if a

portion of all issued, unexpired identification media are lost, stolen, or otherwise unaccounted for, including identification media that are combined with access media.

(vi) Ensure that only one identification medium is issued to an individual at a time, except for personnel who are employed with more than one company and require additional identification media to carry out employment duties. A replacement identification medium may only be issued if an individual declares in writing that the medium has been lost, stolen, or destroyed.

(b) *Temporary identification media.* Each airport operator may issue personnel identification media in accordance with its security program to persons whose duties are expected to be temporary. The temporary identification media system must include procedures and methods to—

(1) Retrieve temporary identification media;

(2) Authorize the use of a temporary media for a limited time only;

(3) Ensure that temporary media are distinct from other identification media and clearly display an expiration date; and

(4) Ensure that any identification media also being used as an access media meet the criteria of § 1542.207(d).

(c) *Airport-approved identification media.* TSA may approve an amendment to the airport security program that provides for the use of identification media meeting the criteria of this section that are issued by entities other than the airport operator, as described in the security program.

(d) *Challenge program.* Each airport operator must establish and carry out a challenge program that requires each individual who has authorized unescorted access to secured areas and SIDA's to ascertain the authority of any individual who is not displaying an identification medium authorizing the individual to be present in the area. The challenge program must include procedures to challenge individuals not displaying airport approved identification media. The procedure must—

(1) Apply uniformly in secured areas, SIDA's, and exclusive areas;

(2) Describe how to challenge an individual directly or report any individual

not visibly displaying an authorized identification medium, including procedures to notify the appropriate authority; and

(3) Describe support of challenge procedures, including law enforcement and any other responses to reports of individuals not displaying authorized identification media.

(e) *Escorting.* Each airport operator must establish and implement procedures for escorting individuals who do not have unescorted access authority to a secured area or SIDA that—

(1) Ensure that only individuals with unescorted access authority are permitted to escort;

(2) Ensure that the escorted individuals are continuously accompanied or monitored while within the secured area or SIDA in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted, and to take action in accordance with the airport security program;

(3) Identify what action is to be taken by the escort, or other authorized individual, should individuals under escort engage in activities other than those for which access was granted;

(4) Prescribe law enforcement support for escort procedures; and

(5) Ensure that individuals escorted into a sterile area without being screened under § 1544.201 of this chapter remain under escort until they exit the sterile area, or submit to screening pursuant to § 1544.201 or § 1546.201 of this chapter.

(f) *Effective date.* The identification systems described in this section must be implemented by each airport operator not later than November 14, 2003.

§ 1542.213 Training.

(a) Each airport operator must ensure that individuals performing security-related functions for the airport operator are briefed on the provisions of this part, Security Directives, and Information Circulars, and the security program, to the extent that such individuals need to know in order to perform their duties.

§ 1542.215

(b) An airport operator may not authorize any individual unescorted access to the secured area or SIDA, except as provided in §1542.5, unless that individual has successfully completed training in accordance with TSA-approved curriculum specified in the security program. This curriculum must detail the methods of instruction, provide attendees with an opportunity to ask questions, and include at least the following topics—

- (1) The unescorted access authority of the individual to enter and be present in various areas of the airport;
- (2) Control, use, and display of airport-approved access and identification media;
- (3) Escort and challenge procedures and the law enforcement support for these procedures;
- (4) Security responsibilities as specified in §1540.105;
- (5) Restrictions on divulging sensitive security information as described in part 1520 of this chapter; and
- (6) Any other topics specified in the security program.

(c) An airport operator may not authorize any individual unescorted access to the AOA, except as provided in §1542.5, unless that individual has been provided information in accordance with the security program, including—

- (1) The unescorted access authority of the individual to enter and be present in various areas of the airport;
- (2) Control, use, and display of airport-approved access and identification media, if appropriate;
- (3) Escort and challenge procedures and the law enforcement support for these procedures, where applicable;
- (4) Security responsibilities as specified in §1540.105;
- (5) Restrictions on divulging sensitive security information as described in part 1520 of this chapter; and
- (6) Any other topics specified in the security program.

(d) Each airport operator must maintain a record of all training and information given to each individual under paragraphs (b) and (c) of this section for 180 days after the termination of that person's unescorted access authority.

(e) As to persons with unescorted access to the SIDA on November 14, 2001,

49 CFR Ch. XII (10–1–10 Edition)

training on responsibility under §1540.105 can be provided by making relevant security information available.

(f) Training described in paragraph (c) of this section must be implemented by each airport operator not later than November 14, 2002.

§ 1542.215 Law enforcement support.

(a) In accordance with §1542.217, each airport operator required to have a security program under §1542.103(a) or (b) must provide:

(1) Law enforcement personnel in the number and manner adequate to support its security program.

(2) Uniformed law enforcement personnel in the number and manner adequate to support each system for screening persons and accessible property required under part 1544 or 1546 of this chapter, except to the extent that TSA provides Federal law enforcement support for the system.

(b) Each airport required to have a security program under §1542.103(c) must ensure that:

(1) Law enforcement personnel are available and committed to respond to an incident in support of a civil aviation security program when requested by an aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter.

(2) The procedures by which to request law enforcement support are provided to each aircraft operator or foreign air carrier that has a security program under part 1544 or 1546 of this chapter.

§ 1542.217 Law enforcement personnel.

(a) Each airport operator must ensure that law enforcement personnel used to meet the requirements of §1542.215, meet the following qualifications while on duty at the airport—

(1) Have arrest authority described in paragraph (b) of this section;

(2) Are identifiable by appropriate indicia of authority;

(3) Are armed with a firearm and authorized to use it; and

(4) Have completed a training program that meets the requirements of paragraphs (c) and (d) of this section.

(b) Each airport operator must ensure that each individual used to meet

the requirements of §1542.215 have the authority to arrest, with or without a warrant, while on duty at the airport for the following violations of the criminal laws of the State and local jurisdictions in which the airport is located—

(1) A crime committed in the presence of the individual; and

(2) A felony, when the individual has reason to believe that the suspect has committed it.

(c) The training program required by paragraph (a)(4) of this section must—

(1) Meet the training standard for law enforcement officers prescribed by either the State or local jurisdiction in which the airport is located for law enforcement officers performing comparable functions.

(2) Specify and require training standards for private law enforcement personnel acceptable to TSA, if the State and local jurisdictions in which the airport is located do not prescribe training standards for private law enforcement personnel that meets the standards in paragraph (a) of this section.

(3) Include training in—

(i) The use of firearms;

(ii) The courteous and efficient treatment of persons subject to inspection, detention, search, arrest, and other aviation security activities;

(iii) The responsibilities of law enforcement personnel under the security program; and

(iv) Any other subject TSA determines is necessary.

(d) Each airport operator must document the training program required by paragraph (a)(4) of this section and maintain documentation of training at a location specified in the security program until 180 days after the departure or removal of each person providing law enforcement support at the airport.

§ 1542.219 Supplementing law enforcement personnel.

(a) When TSA decides, after being notified by an airport operator as prescribed in this section, that not enough qualified State, local, and private law enforcement personnel are available to carry out the requirements of §1542.215, TSA may authorize the airport oper-

ator to use, on a reimbursable basis, personnel employed by TSA, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality to supplement State, local, and private law enforcement personnel.

(b) Each request for the use of Federal personnel must be submitted to TSA and include the following information:

(1) The number of passengers enplaned at the airport during the preceding calendar year and the current calendar year as of the date of the request.

(2) The anticipated risk of criminal violence, sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

(3) A copy of that portion of the security program which describes the law enforcement support necessary to comply with §1542.215.

(4) The availability of law enforcement personnel who meet the requirements of §1542.217, including a description of the airport operator's efforts to obtain law enforcement support from State, local, and private agencies and the responses of those agencies.

(5) The airport operator's estimate of the number of Federal personnel needed to supplement available law enforcement personnel and the period of time for which they are needed.

(6) A statement acknowledging responsibility for providing reimbursement for the cost of providing Federal personnel.

(7) Any other information TSA considers necessary.

(c) In response to a request submitted in accordance with this section, TSA may authorize, on a reimbursable basis, the use of personnel employed by a Federal agency, with the consent of the head of that agency.

§ 1542.221 Records of law enforcement response.

(a) Each airport operator must ensure that—

(1) A record is made of each law enforcement action taken in furtherance of this part; and

(2) The record is maintained for a minimum of 180 days.

(b) Data developed in response to paragraph (a) of this section must include at least the following, except as authorized by TSA:

(1) The number and type of weapons, explosives, or incendiaries discovered during any passenger-screening process, and the method of detection of each.

(2) The number of acts and attempted acts of aircraft piracy.

(3) The number of bomb threats received, real and simulated bombs found, and actual detonations on the airport.

(4) The number of arrests, including—

(i) Name, address, and the immediate disposition of each individual arrested;

(ii) Type of weapon, explosive, or incendiary confiscated, as appropriate; and

(iii) Identification of the aircraft operators or foreign air carriers on which the individual arrested was, or was scheduled to be, a passenger or which screened that individual, as appropriate.

Subpart D—Contingency Measures

§ 1542.301 Contingency plan.

(a) Each airport operator required to have a security program under § 1542.103(a) and (b) must adopt a contingency plan and must:

(1) Implement its contingency plan when directed by TSA.

(2) Conduct reviews and exercises of its contingency plan as specified in the security program with all persons having responsibilities under the plan.

(3) Ensure that all parties involved know their responsibilities and that all information contained in the plan is current.

(b) TSA may approve alternative implementation measures, reviews, and exercises to the contingency plan which will provide an overall level of security equal to the contingency plan under paragraph (a) of this section.

§ 1542.303 Security Directives and Information Circulars.

(a) TSA may issue an Information Circular to notify airport operators of security concerns. When TSA determines that additional security meas-

ures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

(b) Each airport operator must comply with each Security Directive issued to the airport operator within the time prescribed in the Security Directive.

(c) Each airport operator that receives a Security Directive must—

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

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

(d) In the event that the airport operator is unable to implement the measures in the Security Directive, the airport operator must submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval. The airport operator must submit the proposed alternative measures within the time prescribed in the Security Directive. The airport operator must implement any alternative measures approved by TSA.

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

(f) Each airport operator that receives a Security Directive or an Information Circular and each person who receives information from a Security Directive or an Information Circular must:

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

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

§ 1542.305 Public advisories.

When advised by TSA, each airport operator must prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures. This information must be posted in the manner specified in the security program and for such a period of time determined by the Secretary of Transportation.

§ 1542.307 Incident management.

(a) Each airport operator must establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

(b) Immediately upon direct or referred receipt of a threat of any of the incidents described in paragraph (a) of this section, each airport operator must—

(1) Evaluate the threat in accordance with its security program;

(2) Initiate appropriate action as specified in the Airport Emergency Plan under 14 CFR 139.325; and

(3) Immediately notify TSA of acts, or suspected acts, of unlawful interference to civil aviation operations, including specific bomb threats to aircraft and airport facilities.

(c) Airport operators required to have a security program under §1542.103(c) but not subject to 14 CFR part 139, must develop emergency response procedures to incidents of threats identified in paragraph (a) of this section.

(d) To ensure that all parties know their responsibilities and that all procedures are current, at least once every 12 calendar months each airport operator must review the procedures required in paragraphs (a) and (b) of this section with all persons having responsibilities for such procedures.

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

Subpart A—General

- Sec.
- 1544.1 Applicability of this part.
- 1544.3 TSA inspection authority.

Subpart B—Security Program

- 1544.101 Adoption and implementation.
- 1544.103 Form, content, and availability.
- 1544.105 Approval and amendments.

Subpart C—Operations

- 1544.201 Acceptance and screening of individuals and accessible property.
- 1544.203 Acceptance and screening of checked baggage.
- 1544.202 Persons and property onboard an all-cargo aircraft.
- 1544.205 Acceptance and screening of cargo.
- 1544.207 Screening of individuals and property.
- 1544.209 Use of metal detection devices.
- 1544.211 Use of X-ray systems.
- 1544.213 Use of explosives detection systems.
- 1544.215 Security coordinators.
- 1544.217 Law enforcement personnel.
- 1544.219 Carriage of accessible weapons.
- 1544.221 Carriage of prisoners under the control of armed law enforcement officers.
- 1544.223 Transportation of Federal Air Marshals.
- 1544.225 Security of aircraft and facilities.
- 1544.227 Exclusive area agreement.
- 1544.228 Access to cargo and cargo screening: Security threat assessments for cargo personnel in the United States.
- 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.
- 1544.230 Fingerprint-based criminal history records checks (CHRC): Flightcrew members.
- 1544.231 Airport-approved and exclusive area personnel identification systems.
- 1544.233 Security coordinators and crewmembers, training.
- 1544.235 Training and knowledge for individuals with security-related duties.
- 1544.237 Flight deck privileges.
- 1544.239 Known shipper program.

Subpart D—Threat and Threat Response

- 1544.301 Contingency plan.
- 1544.303 Bomb or air piracy threats.
- 1544.305 Security Directives and Information Circulars.

Subpart E—Screener Qualifications When the Aircraft Operator Performs Screening

- 1544.401 Applicability of this subpart.
- 1544.403 [Reserved]
- 1544.405 Qualifications of screening personnel.
- 1544.407 Training, testing, and knowledge of individuals who perform screening functions.
- 1544.409 Integrity of screener tests.