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

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

(a) Each airport operator required to have a security program under § 107.103(a) shall establish an AOA, unless the entire area is designated as a secured area.

(b) Each airport operator required to establish an AOA shall 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 systems, measures, or procedures for controlling entry to the AOA of the airport in accordance with § 107.207.

(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 § 107.213(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 shall be posted by each airport operator in accordance with its security program not later than November 14, 2003.

(5) If approved by the Administrator, 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.

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

(a) Each airport operator required to have a security program under § 107.103(a) shall establish at least one SIDA. Each secured area must be a SIDA. Other areas of the airport may be SIDA's.

(b) Each airport operator required to establish a SIDA shall establish and carry out measures to prevent the unauthorized presence and movement of individuals in the SIDA and shall do the following:

(1) Establish and carry out a personnel identification system described under § 107.211.

(2) Subject each individual to employment history verification as described in § 107.209 before authorizing unescorted access to a SIDA.

(3) Train each individual before granting unescorted access to the SIDA, as required in § 107.213(b).

§ 107.207 Access control systems.

(a) *Secured area.* Except as provided in paragraph (b) of this section, the systems, measures, or procedures for controlling entry to the secured area required under § 107.201(b)(1) shall—

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

(c) *Air operations area.* The systems, measures, or procedures for controlling entry to the AOA required under § 107.203(b)(1) shall incorporate accountability procedures to maintain their integrity.

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

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

(1) Verifies the authorization of the individual to have unescorted access to secured areas or AOAs;

(2) Restricts the time period of entry with the second access medium;

(3) Retrieves the second access medium when expired;

(4) Deactivates or invalidates the original access medium until the individual returns the second access medium; and

(5) Provides that any second access media that is also used as identification media meet the criteria of §107.211(b).

§107.209 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 §107.31 (n) as it existed before 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 §108.229 of this chapter making a certification under this section.

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

(c) *Individuals who have not had a CHRC.* (1) Except as provided in paragraph (m) of this section, each airport operator must ensure that after December 6, 2002, no individual retains unescorted access authority, unless the airport operator has obtained and submitted a fingerprint under this part.

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

(d) *Disqualifying criminal offenses.* An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the disqualifying crimes listed in this paragraph 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.