DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 107 and 139

[Docket No. FAA–2001–8724; Formerly Docket No. 28979; Amendment No. 107–13, 139–23]

RIN 2120–AD46

Airport Security

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This final rule amends the existing airport security rules. It revises certain applicability provisions, definitions, and terms; reorganizes these rules into subparts containing related requirements; and incorporates some requirements already implemented in security programs. This revision also incorporates certain new measures to provide for enhanced airport security. Specifically, this final rule more clearly defines the areas of the airport in which security interests are the most critical and where security measures should be the most stringent. The intent of this final rule is to enhance security for the traveling public, aircraft operators, and persons employed by or conducting business at public airports by increasing awareness of and compliance with civil aviation security measures.

EFFECTIVE DATE: November 14, 2001.

FOR FURTHER INFORMATION CONTACT: Robert J. Cammaroto, Office of Civil Aviation Security Policy and Planning, Federal Aviation Administration, 800 Independence Ave., SW., Washington, DC 20591; telephone (202) 267–7723.

SUPPLEMENTARY INFORMATION:

Availability of Final Rule

You can get an electronic copy using the Internet by taking the following steps:

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

(2) On the search page type in the last four digits of the Docket number shown at the beginning of this notice. Click on ''search.''

(3) On the next page, which contains the Docket summary information for the Docket you selected, click on the final rule.

You can also get an electronic copy using the Internet through FAA's web page at http://www.faa.gov/avr/armhome.htm or the **Federal Register**'s web page at http://www.access.gpo.gov/su_docs/aces/aces140.html.

You can also get a copy by submitting a request to the Federal Aviation Administration, Office of Rulemaking, ARM–1, 800 Independence Avenue, SW, Washington, DC 20591, or by calling (202) 267–9680. Make sure to identify the amendment number or docket number of this final rule.

Small Business Regulatory Enforcement Fairness Act

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires FAA to comply with small entity requests for information or advice about compliance with statutes and regulations within its jurisdiction. Therefore, any small entity that has a question regarding this document may contact their local FAA official, or the person listed under **FOR FURTHER INFORMATION CONTACT.** You can find out more about SBREFA on the Internet at our site, http://www.faa.gov/avr/arm/sbrefa.htm. For more information on SBREFA, e-mail us 9-AWA-SBREFA@faa.gov.

Background

The FAA published a proposed rule on airport security on August 1, 1997 (62 FR 41760; Notice No. 97–13). On the same date, the FAA issued Notice 9712 to revise part 108, Aircraft Operator Security (62 FR 41730). The crash of TWA 800 on July 17, 1996 raised concerns about the safety and security of civil aviation, leading the President to create the White House Commission on Aviation Safety and Security, headed by the Vice President. The Commission issued an initial report on September 9, 1996, with 20 specific recommendations for improving aviation security. On February 12, 1997, the Commission issued its Final Report with 57 recommendations, 31 of which deal with improving aviation security for travelers. In addition, the Federal Aviation Reauthorization Act of 1996 (Pub. L. 104–264) was signed on October 9, 1996, and directs the FAA to amend rules to upgrade civil aviation security.

The FAA has been working to respond to the recommendations of the Commission and to carry out the legislation, and has issued several proposals, in addition to the proposed rule put forth in Notice No. 97–13. On September 24, 1998, the FAA issued a Final Rule on employment history, verification, and criminal records checks. (63 FR 51218; September 24, 1998).

The rules proposed in Notice No. 97–13 were not written in response to the Commission or the Reauthorization Act. Rather, the notice, which proposed to update the overall regulatory structure for airport and aircraft operator security, involved the FAA, other Federal agencies and commissions, airports and aircraft operators, and the Aviation Security Advisory Committee (ASAC). Nevertheless, the extensive proposed revisions were considered to be consistent with the intentions of the mandates, contained proposals industry had identified as necessary or appropriate, and outlined a new organization for the regulations that would assist in developing future changes to the rules. For these reasons, the FAA published the proposed rule for comment. This final rule addresses comments to that proposal.

The revision of part 108, published concurrently with this rule, contains a discussion of the current terrorist threat that also is applicable to concerns under part 107.

The Role of the ASAC

On April 3, 1989, the Secretary of Transportation announced the formation of a national ASAC under the provision of the Federal Advisory Committee Act (Title 5 U.S. Code, Appendix II).

The ASAC was formed to examine all areas of civil aviation security and to ensure a higher degree of safety for the traveling public by recommending improvement of aviation security equipment and procedures. The ASAC is chaired by the FAA's Assistant Administrator for Civil Aviation Security and makes recommendations to the FAA Administrator. Committee membership represents a balance of Federal government, aviation industry, and consumer advocacy groups.

All ASAC meetings are open to the public and are announced in the **Federal Register**. Meetings typically are held three times a year. Members of the public are permitted to attend and appear before the committee, subject to reasonable limitations of space and time.

In December 1993, the FAA sought the ASAC's comments on a ''discussion paper'' that included a broad range of security issues and concerns. A copy of this paper is filed in the FAA public docket for Notice No. 97–13 (Docket No. 28979).

To address the issues raised in the discussion paper, the ASAC formed two subcommittees, and developed recommendations on airport and aircraft operator security issues, which were reported to the FAA on March 15, 1994. Individual ASAC members also provided comments on issues when their respective organizations disagreed with the position of the committee.

Then the ASAC's and individual committee members' comments were forwarded to the FAA with an overall recommendation that security regulations should remain flexible and contain only general security performance standards.

General Discussion of the Rule

The FAA is required to prescribe rules as needed, to protect persons and property on aircraft against acts of criminal violence and aircraft piracy, and to prescribe rules for screening passengers and property for dangerous weapons, explosives, and destructive substances (*See* 49 U.S.C. 44901 through 44904).

To comply with the statute, the FAA has issued rules that require airport operators to perform various duties to ensure the security of civil aviation. Title 14, Code of Federal Regulations, contains part 107 that is directed specifically toward airport operators, and contains general requirements for promoting civil aviation security.

Airport operators are required by new § 107.101 to have a security program, approved by the Administrator that specifies measures they will use to perform their regulatory and statutory responsibilities. The airport security program contains sensitive security information (SSI) and is available only to persons with a need-to-know. Most airport security programs include the following information: descriptions of the air operations area (AOA), each area on or adjacent to the airport that affects the security of the AOA, and air carriers exclusive areas; procedures to control access to the AOA; alternate security procedures for use in emergency and other unusual conditions; and law enforcement support training and record maintenance programs in furtherance of part 107. Programs for some airports include a description of the law enforcement support training program and the system for maintaining records.

Other sources of information and measures are contained in Security Directives and Information Circulars described in new § 107.303. These sources address threats to civil aviation security as well as responsive measures to those threats.

The airport security program is far more detailed than the regulations and, therefore, there will be items specifically addressed in detail that may only be broadly addressed in the regulatory language of part 107. Once approved, the security program has the force of law, and like the part 107 regulations, airport operators must comply with their security program.

This revision of part 107 comprehensively updates airport security regulations to more efficiently and effectively address terrorist and other criminal threats to civil aviation. This action incorporates procedures currently in security programs into part 107, in a manner that is intended to allow regulated entities and individuals to better understand their respective security responsibilities. Concurrent with the issuance of this final rule, the FAA is updating relevant guidance that will help to ensure that airport security programs are consistent with this rule. Lastly, the final rule incorporates certain new measures that will provide for enhanced security. For example, the revisions make individuals directly accountable to the FAA for non-compliance with certain regulations.

Furthermore, local authorities will not be prevented from also taking action against an individual for non-compliance with the regulation, even if the FAA previously has taken action against that individual for the same offense. In fact, the FAA realizes that some local actions may be imposed more quickly and effectively than the agency's actions.

The proposal would have required that an airport's security program include specific local disciplinary actions and penalties for employees who do not comply with security requirements. Initially, this proposal was quite controversial. However, the public's opinion regarding this issue apparently has changed. In response, the FAA reopened the comment period from August 10–September 24, 1999, to receive additional comments from the public on the individual accountability issue [64 FR 43321 (August 10, 1999)]. Therefore, the FAA will not address this issue in this final rule, it will be addressed in a future rulemaking.

Through these changes, the FAA hopes to create a more effective mix of individual and corporate responsibility for complying with security regulations, particularly those relating to access controls and challenge procedures.

General Discussion of the Comments

The NPRM initially requested comments by December 1, 1997. Two public meetings were announced on October 15, 1997, in Washington, DC, and on October 22, 1997, in Fort Worth, TX. On April 14, 1998, the FAA reopened the comment period and announced two public meetings on the NPRM. The public meetings were held on May 21, 1998, in Washington, DC, and June 4, 1998, in Nashville, TN.

As of June 26, 1998, the closing of the second comment period, about 200 comments were received addressing the NPRM. Comments were received from 62 airports, two State and local governments, four law enforcement entities, eight air carriers, and seven industry associations representing these interests. Comments were also received from numerous individuals.

Secured Area, Air Operations Area (AOA), and Security Identification Display Area (SIDA)

Proposal: Notice 97–13 proposed to change the names of the various areas controlled under part 107, and to make some changes in the security measures that apply to each. Under the current rule there are several areas that have been introduced over the years for various security purposes.

Security measures have been required in the AOA since the inception of part 107 in 1972. The definition of AOA in current § 107.1(b)(2) is ''a portion of an airport designed and used for landing, takeoff, or surface maneuvering of airplanes. * * *'' Current § 107.13 provides the security requirements for the AOA. Basically, the airport operator must use the measures in its security program to control access to the AOA and prevent entry of unauthorized persons and ground vehicles; to control movement of persons and ground vehicles, including display of ID when appropriate; and to detect and control each unauthorized penetration.

The secured area was introduced in 1989 in § 107.14. Its location on airports intentionally was not defined to avoid compromising airport operators' security programs. See 54 FR 582 at 584 (January 6, 1989). Section 107.14 requires enhanced access controls for secured areas of the airport mostly using computerized access controls. This area for most airports has evolved to be mainly portions of the AOA near the terminal and in baggage make-up areas, where the highest levels of security are needed. For some airports, the entire AOA is a secured area, because of such factors as the location of the airport and the inability to use adequate security controls to separate general aviation and other areas from air carrier operations.

The SIDA was defined in 1991. The SIDA is defined in current § 107.25(a) as ''any area identified in the airport security program as requiring each person to continuously display on their outermost garment, an airport-approved ID medium unless under airport-approved escort.'' The ID medium is referred to as being used for both access control and controlling the presence and movement of persons. The portions of the airport that must be a SIDA are not set out in current part 107. The

preambles to proposed and final § 107.205, however, indicate that SIDA generally would include secured areas (§ 107.14), air operations areas (§ 107.1(b)(2)), cargo and baggage make-up areas, and other areas specified in individual airport security programs. SIDA would not include the sterile area. There also would be site-specific provisions at those airports where general aviation and other areas are positively separated from air carrier operations [56 FR 13552 at 13553, and 56 FR 41412 at 41413]. Thus, the secured area, part or all of the AOA, and some areas that are neither secured areas nor AOA (such as some cargo makeup areas) could be within a SIDA. The security measures required in the SIDA are in §§ 107.25 and 107.31. These sections require training of persons with unescorted access to the SIDA, and employment history, verification, and criminal history records checks of those persons.

This systematic design of interlocking areas has created some confusion in the past. It has not been clear where the limits of the secured area should be, for instance. Notice 97–13 attempted to propose a design that would be simpler and clearer. It proposed to eliminate overlapping areas, such as where both the AOA rules and the secured area rules apply. It also proposed, based in part on recommendations from the ASAC, to rename the areas so that what is now the secured area would be the critical security area (CSA), and what is now the AOA outside of the secured area would be the restricted operations area (ROA). Definitions of these terms were proposed in § 107.3. Sections 107.201 and 107.203 proposed specific requirements for access systems, ID systems, and other security measures to be applied in the CSA and ROA, respectively. The intent was to more clearly describe those areas of the airport in which the security interests are the most critical and require the most stringent measures, and to enhance the security of other parts of the ROA.

Comments on changing the names of the areas: Many commenters object to changing the names of the secured area, AOA, and SIDA. They state that the industry has become familiar with these names and that changing them now would create confusion. It would also result in very large expenses to change training programs and videos, airport manuals, emergency plans, signs, and many other items. The commenters note that spending a significant amount of time, effort, and funds on retraining, signs, documentation, and security programs for renaming the above noted areas, would not improve security. The commenters strongly urge that the names not be changed.

One commenter suggests that acronyms for defined terms should be included in the definitions. Another commenter says that the FAA should avoid using 3-letter acronyms that replicate an airport's 3-letter designator code.

FAA response: The FAA has decided not to change the names of the areas to CSA and ROA. After further consideration, changing these names would create a burden to change numerous documents, signs, training programs, and the like with insufficient benefit. The industry has become used to these names and there is not the same concern there was several years ago about them.

Regarding the use of acronyms, the FAA will adopt the suggestion to reference commonly used acronyms in the definitions. Also, in response to the comment on acronyms relating to security terms as opposed to 3-letter airport designator codes, the FAA notes that security terms and their acronyms are based on functional descriptions of what they are intended to define. The FAA's system of 3-letter airport designator codes is a separate and distinct program. The agency recognizes that some acronyms and 3-letter airport identifiers may be unintentionally identical, but it is not aware of any conflicts at this time. However, it is expected that the context in which overlapping terms would be used will indicate their intent.

Comments on definitions of critical security area, restricted security area, secured area, AOA, and SIDA: National Air Transport Association (NATA) and Missoula International Airport comment that areas used by general aviation should be excluded from the critical security area and maintained in the AOA, and have less intrusive security requirements. The ATA requests a definition of ''AOA.'' Several commenters including three airports requested a definition of ''SIDA.''

The Port Authority of NY and NJ suggests that ''critical security area'' should be defined as ''where aircraft operators and foreign aircraft operators enplane and deplane passengers and sort and load baggage and any *immediately* adjacent areas that are not separated by security controls, physical or visual barriers, adequate time and distance separation or visual surveillance.''

Atlanta Hartsfield International Airport requests that the FAA add the phrase ''time and distance'' after the phrase ''physical barriers'' in the definition of ''restricted operations area.'' Furthermore, Ft. Wayne Airport suggests the definition should be modified to include *only* areas that are used by aircraft operators for the carriage of passengers. Another commenter says that the restricted operations area should allow the use of ''visual barriers,'' such as lines or words painted on the pavement.

One commenter requests clarification of the phrases ''adjacent areas'' and ''other security measures'' which are used in the definition of ''critical security area.''

The NATA requests a definition of the area of an airport where general aviation activities occur. One suggestion is to define the term ''General Aviation Security Area'' so that the general aviation areas are not included in the critical security area or restricted operations area.

Two airports state that the ROA should be defined and limited to only those areas outside the critical security area and immediately adjacent to facilities needed for aircraft operators to land, depart, taxi, park, and maneuver aircraft. All other areas should be considered non-restricted AOA portions of the airport and a definition for an AOA included in the new part 107. The proposed rule, as written, would require a massive expenditure of critically needed funds to extend and upgrade the systems presently installed.

The Airport Council International-North America (ACI–NA), American Association of American Executives (AAAE), and two airports state that increasing the size of the restricted operations area directly contravenes the recommendations of the ASAC working group.

FAA Response: This rule adds definitions to better describe the limits of the secured area, AOA, and SIDA. These definitions in part are intended to conform part 107 to what has become common practice in determining the limits of these areas at airports. The FAA anticipates that there will be few changes needed in the boundaries of current secured areas, SIDAs, and AOAs based on these rule changes, although nationwide we anticipate a small reduction in the current security areas and corresponding increase in the AOA. These definitions reduce the overlap between the areas by clearly separating the AOA from the secured area. Each will be a distinct area, with different requirements. This assists in accomplishing the goal of providing for the highest levels of security at those places where operations regulated under parts 108 and 129 are conducted.

The secured area is that area where the highest level of security measures

are needed. This includes areas where part 108 operations enplane and deplane passengers and sort and load baggage, and adjacent areas that are not separated by adequate security measures. Unlike the current rule, the term ''secured area'' is not used only to describe the area where enhanced access controls are required. It is used to describe an area where a range of enhanced security measures are required, including identification media, escort, and challenge programs. This is consistent with current practice. For example, those areas in which the enhanced access controls are considered necessary are also SIDAs with ID display required.

The SIDA is essentially not changed from the current rule. It overlays secured area, in that the secured area must be a SIDA. It may overlap an AOA, in that at some airports it may be necessary for part or all of the AOA to be a SIDA. The SIDA may also be in an area outside of either the secured area or AOA, such as a cargo makeup area. The security measures required for the SIDA have not been changed significantly.

The AOA is almost the same concept as used in current part 107, except that it is limited to those areas that are used by parts 108 and 129 operations, and those adjacent areas that are not separated by adequate security measures. Further, the secured area is no longer considered part of the AOA. The security measures required in the AOA include controlling access and presence of unauthorized persons and vehicles. There remains flexibility as to exact measures to be used to accomplish these tasks, because each airport is different and may have different needs in the AOA. For instance, personnel ID systems may or may not be used in the AOA.

The proposal used the phrase ''any adjacent areas that are not separated by security controls or physical barriers.'' The final rule uses the phrase ''adjacent areas that are not separated by adequate security systems, measures, or procedures.'' Physical barriers are one sort of security measure, and may be a critical part of a security system that permits an adjacent area to be excluded from a secured area or an AOA. There are many other provisions that in appropriate combinations may provide adequate security systems, measures, or procedures. They include remoteness from the adjacent operation (''time and distance'') combined with specific measures to detect and respond to unauthorized penetrations, fences, personnel ID systems, closed circuit TV, clear markings, and security patrols. Given the wide variations in airports and the various security systems in use, it is impossible to state specifically in the rule what is needed at each airport. Further, much of the information on the security systems to be used at each airport must be kept non-public to avoid giving unauthorized persons information that could be used to attempt to defeat them.

As to signs, markings, and visual barriers, it must be noted that these are effective mostly for people who are attempting in good faith to comply with the security systems at the airport. Standing alone, they are not very effective at keeping out persons who are intending to defeat the system.

The FAA considered using the term ''immediately adjacent,'' rather than just ''adjacent.'' However, this might be viewed as too limiting. The key is whether the adjacent area can be separated by adequate security measures. Distance alone is not sufficient. For instance, to be effective, distance must be coupled with adequate measures to detect and respond to unauthorized persons attempting to cross that distance. In each case, the airport operator and the FAA must consider not only how close the adjacent area is, but also what security measures are present, what related activity is in the area, and all other factors. It is impossible to state specifically how far an area might extend before it is excluded from the secured area or the AOA. For instance, at airports where general aviation (GA) activity is sufficiently remote from the secured area and there are dedicated measures to detect and challenge persons moving from the GA area to the secured area, that GA area may not need to be included in the secured area. At other locations where the GA activity is close to the terminal, and it is not possible to erect adequate physical barriers, there may be no way to provide adequate security measures to exclude the GA area from the secured area. Removing GA areas from the AOA, this too depends on the airport. GA areas are usually near taxiways and/or runways used by parts 108 and 129 aircraft, and are usually within the perimeter fence of the airport. Even if a GA area is remote from the secured area it may not be possible to have adequate security measures to omit it from the AOA. However, if the GA area is separated from the taxiways and runways by a fence and controlled gate, there may be a basis to exclude it from the AOA. Again, the FAA does not consider the secured area and AOA, as defined in the final rule, to be vastly different than what currently exists at the airports. This final rule to a large extent more clearly reflects the areas as they have evolved from the more general and vague language of the current rule.

The security measures required in each area are discussed more fully in the Section-by-Section Analysis.

The Notice did not propose to retain the term SIDA. As discussed above, the FAA has decided to retain this term, with modifications. As used in current § 107.25, SIDA refers to ''any area identified in the airport security program as requiring each person to continuously display on their outermost garment, an airport-approved identification medium unless under airport-approved escort.'' It was based on the idea that, if the area was of such an importance to security to have a requirement in the security program for the continuous display of identification, it should also have the training requirements in § 107.25 to ensure that airport personnel know their duties to challenge persons without ID, and the employment verification of § 107.31.

This final rule changes the definition of SIDA to ''a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport, such as areas where there are activities related to the operations of aircraft operators and foreign air carriers that have security programs under part 108 or § 129.25 of this chapter.'' This definition is intended to capture the original intent of the SIDA. It includes the secured area, in which the highest level of security is required. An airport operator may include in the SIDA other areas, such as cargo makeup areas, fuel farms, and other areas, particularly where activities related to part 108 and part 129 operations are carried out. On some airports the entire AOA may be designated a SIDA. Again, because of the varied configuration of airports it is not possible to describe exactly the limits of the SIDA.

New § 107.205 states the security measures that must be carried out in the SIDA, and is discussed in the Section-by-Section Analysis.

A strict reading of current § § 107.25 and 107.31 would suggest that any area in which continuous display of ID is provided for in the security program also requires the more extensive training in escort and challenge procedures, and employment verification in these sections. It has become evident to the FAA that there are areas of airports outside of the secured area in which, due to local circumstances, the continuous display of ID is required by

local rule, but that do not necessarily warrant the higher security requirements of a SIDA. Examples include areas used exclusively by an aircraft manufacturer or other private corporation, in which continuous display of a corporate ID is required largely for corporate security purposes. Such areas are described in the airport security program because they are part of the overall security situation at the airport. For instance, the airport would make sure that the color and appearance of the corporate ID was not confusingly similar to that of the airport IDs used in the SIDA. The corporate areas, however, need not have all the measures that apply to the SIDA. Nevertheless, the definition as it appears in current part 107 could be read to mean that such areas must be formal SIDA's. New § 107.203(b)(5) acknowledges that such areas may exist in the AOA without them being deemed SIDA's under new § 107.205.

The Notice proposed, in essence, that the CSA (now the secured area) would have all the attributes of the SIDA, with full training and employment verification. The proposed ROA (now AOA) would have ID display required, but not have the same extensive training or employment verification as the SIDA. The final rule represents a middle ground between the current rule and the proposal by requiring the secured area to be a SIDA, and providing the option of less burdensome ID requirements in the AOA.

Time Limits

Proposal: The Notice proposed various time limits for carrying out various tasks, such as approval of a security program, amendments to security programs, and changed conditions affecting security. These tasks were presented with deadlines that were in terms of calendar days and hours.

Comments: A commenter states that compliance timeframes should be adjusted to reflect realistic opportunities. The recommendation was made that the FAA refer to ''business days'' versus a specified number of hours when setting deadlines for compliance.

FAA response: Regarding the use of business days in favor of a specific number of hours, the FAA notes that its regulations usually deal in terms of calendar days or hours (for instance, 30 days or 72 hours). When setting deadlines for compliance the FAA will set reasonable deadlines, based on circumstances, while taking into account holidays and weekends. In emergency situations, it may not be in the interest of security to delay compliance for a weekend or holiday. The agency sees no need to alter its practice. Further, the use of ''business days'' can be confusing. Most airports are open for business every day of the week, including holidays. Further, the observance of holidays is not uniform throughout the country.

Compliance Dates

Proposal: The Notice requested comments regarding compliance dates.

Comments: ACI–NA and AAAE comment that the FAA should provide sufficient time following issuance of a final rule for airports to be in compliance. A minimum phase-in period of 18 months was suggested.

FAA response: The FAA believes this final rule has allowed adequate time for airports to comply. The agency notes that the complexities involved in compliance, as well as anticipated costs, are carefully weighed when deadlines are established. Where difficulties are encountered, airport operators are encouraged to contact their local FAA security field office. The FAA has attempted to ensure a realistic approach to compliance timeframes but recognizes that such timeframes are sometimes not met for good cause. The agency is prepared to extend reasonable consideration when the merits of a situation warrant.

The final rule has far fewer required changes than the NPRM. For instance, the boundaries and names of the secured area, AOA, and SIDA will change little, if at all. Also, some new requirements have intended compliance dates such as for AOA training under § 107.213(c) and (f).

Security Requirements Based on Size of Aircraft Served

Comments: One commenter states that increased airport security thresholds should not be based on the size of the aircraft serving an airport, but on the number of passengers screened annually. One commenter agrees with the statement that experience shows airports served by smaller aircraft need not comply with all of the requirements imposed on larger airports. However, security should be a function of the nature of the service resident at an airport; that is, medium and large hub airports are of more concern, so operations to and from them should be of more concern. The commenter suggests that perhaps the analysis should focus on city pairs instead; and further still, to more highly threatened city pairs. Aircraft sizes and their variations do not, in themselves, create security issues.

FAA response: The agency understands the commenters' concerns about appropriate measures as determined by the size and threat level of particular airports. But, contrary to the comments, the FAA believes that aircraft size and capabilities affect their desirability as targets of terrorism or other criminal acts. Such criteria have historically proven good indicators of where and how to focus limited security resources. There are some requirements that may vary based on the amount of activity at the airport and other factors, which are set out in the individual airport's security programs.

Supplemental Notice of Proposed Rulemaking (SNPRM)

Comments: The ACI–NA and AAAE strongly urge the FAA not to implement the proposed rule until the FAA publishes an SNPRM and reviews the comments. It would be appropriate within this timeframe to examine ways that the ASAC, or a new working group within the ASAC, could be appointed to clarify and streamline this proposal.

Twenty-four airports, an air carrier, a local government, five local departments, and commissions recommend that the FAA publish an SNPRM.

Many commenters state that the FAA states throughout the NPRM that it is an incomplete proposal, and notes that additional language will be supplied at a later, unspecified date.

FAA response: Having received a vast amount of public and industry input to this proposal, and in view of the many changes reflected in the final rule, the FAA is confident that the rule can go forward without the issuance of an SNPRM that covers the entire part 107. This decision is based partly on the fact that the FAA has agreed with many of the issues the commenters felt most strongly about, such as renaming the airport areas. As to another issue of common concern, compliance programs in proposed § 107.103(a)(2) as mentioned under General Discussion of the Rule, the agency reopened the comment period.

The proposal and the final rule, as well as extensive historical experience, make it clear that many specifics of the design and implementation of security programs are not appropriate for the public rulemaking process. The FAA has carefully and diligently indicated the difference between public requirements of the regulation, and specific information that can only appear in the security program. The specific details of security measures, in order to be effective, must often be held closely by those with a ''need to know.''

Since many of the requirements of this final rule have been in place at airports in one form or another for many years, the FAA does not anticipate any regulated parties would be unduly or unnecessarily inconvenienced in complying with them.

Section-by-Section Analysis

The following is a discussion of comments and FAA responses for each proposed section.

Section 107.1 Applicability

The NPRM proposed to extend airport security requirements to airports regularly serving any aircraft operator required to have a security program under parts 108 or 129. This would be a change from the current rule, which covers airport operators regularly serving scheduled operations of aircraft operators required to have a security program. The increase would be those airports that only regularly serve certain public charter operations. The NPRM also proposed to extend the applicability of existing § 107.1 to individuals entering or in critical security areas, restricted operations areas, and sterile areas.

Under proposed § 107.1(b), the term ''Assistant Administrator for Civil Aviation Security'' would be used, rather than the existing ''Director of Civil Aviation Security.'' This position would be defined as the official who oversees civil aviation security operations and approves security programs. In addition, § 107.1(b) would clarify that the Deputy Assistant Administrator for Civil Aviation Security, or any individual formally designated, could act in the capacity of the Assistant Administrator and the duties of this position could be further delegated.

Comments: A commenter states that smaller regional airports do not have staff to perform all requirements in the proposed rule. The FAA would have to fund the salaries of additional personnel so that the facility could comply with the rule.

Another commenter recommends removing the reference to ''sterile area'' in § 107.1(a)(3), as it is controlled by part 108 rules.

Finally, Air Transport Association (ATA) comments that the delegation of the Administrator's authority should be narrowly circumscribed due to the potential for conflicting and overlapping authority.

FAA response: In the past, the FAA generally chose to hold only the airport operator accountable for the actions of persons under its control, with the expectation that corrective actions taken by airport operators would discourage employees and others from repeated non-compliance. The FAA continues to believe that corporate accountability is key to achieving and maintaining compliance. However, the agency also believes that the concept of holding individuals accountable for security violations, in a timely fashion, is a worthy one. The agency remains committed to broadening accountability and the final rule reflects that under new § 107.11.

In response to the comment regarding the lack of staff at smaller regional airports, the FAA refers to the Regulatory Evaluation. Economic analyses are based on estimates which anticipate costs associated with all sizes of airports, and recognizing the costs of the different levels of security measures associated with each.

Regarding removal of the term ''sterile area'' from § 107.1(a)(3), that term originated in part 108, and is used in part 107 to define locations at which a person is subject to individual responsibility for their conduct under this part. The FAA, therefore, has decided to leave the proposed language unchanged while the definition of ''sterile area'' is retained in part 108.

In response to ATA's comment about the delegation of the Administrator's authority, the FAA notes that the proposal reflects the manner in which the FAA's internal chain of command carries out its statutory responsibilities. The FAA agrees that delegations must be carefully evaluated to avoid unnecessary conflicts of authority.

Section 107.3 Definitions

The FAA proposed a new definitions section (§ 107.3) which would include revised definitions from the current part 107. Section 107.3 also would add several new definitions. Existing § 107.3, Security Program, would be incorporated under proposed Subpart B, Airport Security Program. The FAA proposed that the terms defined in part 108, e.g., ''sterile area,'' would apply to this part.

The proposals regarding the secured area, AOA, SIDA, CSA, and ROA are discussed under the General Discussion above. In addition, the FAA proposed the following in § 107.3. The definition of ''exclusive area'' in existing § 107.1 would be revised and grouped with a newly defined ''exclusive area agreement.'' Under the proposal, the definition of ''escort'' was revised to include a reference to the proposed critical security area and restricted operations area. The definition ''sterile area'' was revised in the proposal to clarify the responsibility to conduct inspections of persons and property.

The FAA also proposed adding the following definitions: ''airport security program,'' ''airport tenant,'' ''airport tenant security program,'' ''Assistant Administrator,'' ''exclusive area agreement, ''and ''unescorted access authority.''

Comments on definitions in general: The Regional Airline Association (RAA), Federal Express (FedEx), eight airports, an air carrier, and a local department of aviation request that the FAA define terms more clearly, or continue using the current terms. The commenters also provide detailed suggestions on how to more clearly define some of the terms.

United Parcel Service (UPS), Alaska Airlines, Trans World Airways (TWA), Port Authority of NY and NJ, and Phoenix Aviation Department suggest incorporating the same definitions in parts 107 and 108.

FAA response: Clarity of definitions is a fundamental goal of this rulemaking. In response to RAA, FedEx, and the many other commenters who offered comments on exactly how to go about that task, the FAA wishes to assure them that every effort has been made for clarity and distinctness. The challenge was to develop clarity, while at the same time providing flexibility to allow for local applications and unique circumstances.

As to the requests to repeat the definition of terms used in both parts 107 and 108, the FAA has decided to retain the definitions in the most applicable part. Cross references will indicate that the terms apply to the other part as well. Although it might be more convenient for some users to have the definitions repeated in each part, there is a risk that the definitions would become inconsistent as parts are individually amended from time to time.

Comments on ''escort'': The ATA states that the term ''escort'' should not apply to employees temporarily without aircraft operator identification media.

The UPS and three airports state that the proposed definition of ''escort'' leaves too much room for interpretation. Airport commenters state that the phrase ''sufficient to take action'' is unclear. The FAA should add language that holds individuals accountable for being in direct physical control of persons under escort.

FAA response: In consideration of the comments, the FAA has revised the definition of escort. The term ''escort'' now means ''to accompany or monitor the activities of an individual who does not have unescorted access authority

into or within a secured area or SIDA.'' This emphasizes the primary function of the escorter—to determine whether the escortee is limiting his or her activities to those authorized. If the escortee departs from authorized activities, the escorter would take action in accordance with the security program. This could include verbally challenging the individual, summoning a supervisor, or summoning law enforcement. The minimum requirements for the local design and implementation of escort procedures are set forth in new § § 107.201 and 107.205. Specifics as to where and how this method is to be applied will appear in individual airport security programs. As to the escorter being in ''direct physical control'' of the escortee, this phrase might imply a level of physical control that generally is not needed, such as the level of control a law enforcement officer exerts over a person they have arrested.

Comments on ''exclusive area'': Denver International Airport suggests that the definition of ''exclusive area'' include the concept that now individual access points can be designated as ''exclusive areas.'' The commenter also recommends adding ''located anywhere on the airport'' after the phrase ''access points.''

FAA response: The definition of ''exclusive area'' as proposed was intended to provide the regulated parties with the opportunity to transfer the accountability and responsibilities under part 107 from the airport operator to aircraft operators under parts 108 or 129. The definition as proposed expands the scope of the former definition, which allowed exclusive area agreements only for portions of the AOA. The new definition permits inclusion of portions of an AOA, secured area, and SIDA, which may include access points. For example, a part 108 regulated aircraft operator may now assume specific security responsibilities under part 107 for that portion of the secured area within its leasehold. The aircraft operator may also accept an exclusive area agreement with the airport for part 107 responsibility for any access point (for persons or vehicles) which leads directly into that portion of the secured area. Individual access points may be included in exclusive area agreements in the final rule. Further discussion of exclusive areas appears in response to comments relating to proposed § 107.111.

Comments on ''sterile area'': Several commenters, including three airports, requested that the FAA put the definition of ''sterile area'' in § 107.3 instead of referring the reader to part 108.

FAA response: The definition of sterile area will remain in § 108.3, and will not be repeated in this part. As explained earlier, the FAA has decided to keep the definitions in the most applicable part, with cross-references showing that the terms apply to other parts as well. Section 108.3 states that the term ''sterile area'' means a portion of an airport defined in the security program that provides passengers access to boarding aircraft and to which the access generally is controlled by an aircraft operator or foreign air carrier through the screening of persons and property in accordance with the security program. The use of the term ''sterile area'' in part 107 is for descriptive purposes only.

Comments on ''unescorted access authority'': The Air Line Pilots Association (ALPA) and Juneau International Airport request a definition of ''unescorted access authority.''

Another commenter says that the airport operator should be the only person authorized to grant unescorted access authority.

FAA response: The FAA defines unescorted access authority as the authority granted to individuals to gain entry to, and be present without an escort in secured areas and SIDA's. The FAA disagrees with the comment that only the airport operator should grant unescorted access authority. It has been a longstanding practice for aircraft operators holding security programs under parts 108 or 129 to join with the airport operator in ''exclusive area agreements.'' The intent of such agreements is to transfer certain part 107 requirements to the aircraft operator, as specified in the agreement.

Additionally, it is a common practice for the airport operator to extend or broaden authorization for unescorted access to a class of persons. For example, the acceptance of a particular company's employee identification card, as airport-approved media, effectively extends to such companies the authority to determine who may have such privileges on a case-by-case basis. In each of these cases the airport operator has agreed to extend the privilege to the other party. The FAA believes that as long as a responsible party is empowered to extend that privilege under specific terms, the safety of the flying public can be ensured. Therefore, absent any compelling reasons to the contrary, the FAA will permit parties other than the airport operator to grant unescorted access authority within the constraints of this part.

Comments on clarification of definitions and new definitions: Many commenters request clarification of the following terms: ''media,'' ''vehicle,'' ''person,'' ''physical barriers,'' and ''law enforcement personnel.'' Atlanta Hartsfield International Airport requests clarification of the term ''person.'' A commenter requests a definition of ''physical barriers,'' and recommends including time, distance, or signage in the definition.

The Monterey Peninsula Airport District comments that the FAA should define ''law enforcement personnel'' to consist of state certified police officers. Security guards should supplement, not replace police officers.

FAA response: In response to comments regarding clarification of definitions or the use of new definitions, the FAA notes that it usually does not define terms that are used within their common, everyday meaning. For example, the terms ''media,'' ''ground vehicle,'' and ''physical barriers'' are not used in this rule in unique ways. There is no need to include definitions in the rule.

The term ''media,'' for instance, is used in a conventional sense to identify any means, materials, or techniques that identify an individual or vehicle or convey an individual's access or personnel identification authorization. In common usage, access media can include keys, magnetic cards, or other means to gain entry. In the case of identification media, § 107.211 provides additional standards for such media. The FAA used the term ''physical barriers'' in a conventional sense to include, for example, fences, walls, and buildings. The FAA has not used that term in the final rule, as discussed under Secured Area, AOA, and SIDA, above.

The word ''person'' is already defined in 14 CFR § 1.1. That definition is controlling with regard to part 107 so that there is no reason to repeat that definition in part 107.

Section 107.5 Airport Security Coordinator

The FAA proposed that existing § 107.5, ''Approval of security program,'' would be incorporated into proposed § 107.105, ''Approval and amendments,'' under proposed Subpart B, Airport Security Program. Existing § 107.29, ''Airport Security Coordinator'' would be revised and renumbered as new § 107.5 under new Subpart A, General.

The FAA proposed to further define the functions and responsibilities of the

ASC. The functions of the ASC were discussed in the Employment Standards Rulemaking (56 FR 41412 at 41417–8; August 20, 1991). The FAA also proposed that this section would clarify that an individual serving as an ASC may perform other duties in addition to those required by the FAA, and this need not be the ASC's only duties. It was the FAA's intent to clarify that the ASC requirements did not mandate that airport operators establish additional positions, the duties of which are exclusively security-related. Further, the proposed language was intended to clarify the relationship between the FAA and the ASC.

The FAA also proposed to require training for the ASC every 2 years to ensure that ASC's remain updated on both airport and aircraft operator security regulatory and operational requirements. The FAA requested comments on methods airport operators would use to meet this training requirement.

Lastly, the FAA proposed moving to this section certain provisions of existing § 107.31, recently effective (60 FR 51854; October 3, 1995), regarding the ASC responsibility to review and control results of employment and criminal history checks and to serve as the contact for individuals appealing their results.

Comments on ASC Functions: (Proposed § 107.5(a) and (b)): Cheyenne Airport disagrees with incorporating specific functions and duties of the ASC into the rule. A detailed job description is redundant and unnecessary. Several commenters questioned whether there could be more than one ASC.

FAA response: The FAA's general description of the functions of the ASC reflects the expectation that similar tasks are to be conducted at hundreds of individual airports across the nation. The regulatory framework is considered essential to ensure consistent and reliable understanding of the ASC's duties.

In response to the comments, the final rule clarifies that the airport must have one or more ASC's. This would allow different people to be on call at different times. The FAA anticipates the airport generally will designate a lead ASC, and others who will assist.

Comments on § 107.5(b): One airline commenter says that proposed § 107.5(b)(2) should state that ASC's have contact with Federal Security Managers (FSM), who are FAA special agents, located at certain larger or more complex airports. Another commenter says that the ASC should have contact with the Aircraft Operator Security Coordinator (AOSC) and notes that AOSC's are to be designated at the corporate level.

Atlanta Hartsfield International Airport, Minneapolis Airport, the Port Authority of NY and NJ, Lincoln Airport Authority, and the Phoenix Aviation Department state that the requirement in proposed § 107.5(b)(3) to ''review with sufficient frequency all security related functions'' is vague and leaves a considerable amount of room for interpretation. Denver International Airport states that the phrase ''airport tenant activities'' in this paragraph needs to be defined.

The ACI–NA, AAAE, Atlanta Hartsfield International Airport, Miami International Airport, Tucson Airport, Metropolitan Washington Airports Authority, Capital Region Airport Authority, Lincoln Airport Authority, and Phoenix Aviation Department are under the perception that the ASC would ''perform any duties deemed necessary'' (proposed § 107.5(b)(7)). The commenters believe that this situation would be like leaving a ''blank check'' for the FAA to impose new duties and requirements on the airports; some commenters believe that this paragraph should be deleted and that any additional FAA directed changes should be coordinated and implemented under proposed § 107.107.

FAA response: Regarding the airline comment related to § 107.5(b)(2) that the proposal should state that ASC's should have contact with the FSM, the FAA notes that FSM's are senior FAA civil aviation security specialists whose duties apply specifically to particular airports. Such airports are generally larger and more complex facilities. A FSM is the FAA's designated point of contact for the ASC's at such airports. If there is no FSM for that airport, another contact point from a FAA field office is given to the ASC. Hence, the FAA does not see a need to add or to modify proposed language in this regard.

As to requiring the ASC to contact the AOSC, the AOSC for the aircraft operator is designated at the corporate level, while the ASC is designated at the local airport level. It is not the FAA's intent to require that the ASC communicate with corporate aircraft operator personnel. Generally, the ASC can carry out his or her duties by dealing with their aircraft operator counterpart who is a local Ground Security Coordinator (GSC), as required under part 108. The FAA would prefer to leave the option to contact corporate offices to the airport operator, as it deems necessary.

Regarding § 107.5(b)(3), the FAA disagrees that the proposed language is unduly vague. However, the FAA also recognizes that the scope of airports' security-related functions vary greatly based upon the size and complexity of the markets served by the airport. The proposed language clearly directed the airport operator, through the ASC, to review security functions specified in such documents as the security program, tenant security programs, and applicable Security Directives. These documents are written to a high degree of specificity, and therein lie the details the ASC is expected to review. Hence, the language of the regulation is seen by the FAA to be at the appropriate level of specificity. Consequently, the FAA has chosen to retain in the regulation the broader language with an expectation that more specific requirements will be reflected in or flow from the individual security programs.

In response to Denver International Airport, the FAA notes it has removed the general phrase ''airport tenant activities'' from § 107.5(b)(3). This section has been rewritten to reflect the more specific mandate. The airport operator, through the ASC, must review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with this part and the security program. The agency notes, however, that the security program may include tenant security programs, exclusive area agreements, and other implementing documents. The FAA believes a frequent review of the activities specified in and required by such documents will yield an appropriate level of airport operator oversight and local communications regarding security measures.

The FAA agrees with the many comments about proposed § 107.5(b)(7) that may have implied an unlimited ability of the FAA to add to the duties of the ASC through changes to the security program. Consequently, proposed § 107.5(b)(7) does not appear in this final rule.

Comments on § 107.5(c) Training Schedule and Hours: Anchorage International Airport and Phoenix Aviation Department say that the FAA should host and pay for any ASC training. Port Authority of NY and NJ and Anchorage International Airport say that the FAA should provide initial ASC training and recommends that the AAAE perform recurrent training every 2 years.

The ACI–NA, AAAE, Cheyenne Airport, and Lincoln Airport Authority suggest that biannual training for ASC's at smaller airports is economically burdensome. These commenters add that attendance at training seminars for ASC's at smaller airports is difficult due to tight budgets and limited staff.

Two airports suggest that 180 days after publication of final rule is not sufficient time to be in compliance with such extensive training and recordkeeping and instead recommend a longer compliance date.

FAA response: While the FAA disagrees that it should fund ASC training, it notes that such basic training on the civil aviation security program is available from several sources. For example, the FAA jointly sponsors basic training courses with several industry associations that could provide the ASC with requisite information. Such training, when supplemented with additional information necessary to understand local concerns, would prepare the ASC to carry out the locally defined duties.

The FAA believes that the amount of time necessary for an ASC to receive instruction on the security provisions relevant to their own location would be minimal. Consequently, the FAA does not believe that ASC training comprises an undue burden for any airport.

In response to the last comment above, the FAA accepts that 180 days may be insufficient time for airports to complete training for ASC's. Since training has not been required in the past, it must be developed and budgeted for. The final rule allows for 2 years following the publication date of the rule to achieve compliance with this requirement.

The FAA recognizes the many and valued services currently provided by the nation's ASC's. However, the FAA is also aware that there are inconsistencies in the level of knowledge and experience among ASC's. This variance stems from many factors, such as, tenure in the position, initial training (if any), the individual's current primary duties, and the individual's experience in the performance of ASC duties as well as the individual's background prior to assuming the position. Consequently, the FAA is convinced that baseline training is essential to ensure an adequate level of knowledge of the ASCs.

Therefore, this final rule does not allow for the grandfathering of ASCs as a means to avoid initial training. However, recurrent training is required for only those who have a break in service of 2 years or more during which time the person did not actively perform the duties of a designated ASC. Such persons would have to again take the training to resume ASC duties.

Comments on § 107.5(c) Training Guidance: One airport states that the FAA should formulate guidance materials to clarify airport security issues, and make them available as part of the ASC training. Atlanta International Airport states that ASC training standards should be outlined in an advisory circular (AC) or proposed FAA rule. Lincoln Airport Authority and Port Authority of NY and NJ state that the ASC training curriculum, proficiency standards, and training materials should be developed by the FAA in cooperation with the industry.

Three airports state that the FAA should explain what the ASC training entails.

Two airports suggest that anyone performing in the capacity of the ASC 90 days prior to the effective date of the final rule should be ''grandfathered'' in and not be subject to the basic ASC portions of training. Furthermore, Tucson Airport states that the ASC is the most knowledgeable person at any airport and of the airport's security program and the FAA requirements and, therefore, the retraining of the ASC's basic job skills would be inefficient.

FAA response: The FAA recognizes that the role of the ASC has been expanded. In that context, it is the agency's view that the ASC should be trained to a level of functional familiarity with parts 107, 108, 129, and 191, the airport's relevant operational manuals, the local emergency services support, the process which results in issuances of Security Directives, the security programs (to include contingency plans), and the respective rules and the means to communicate with all airport tenants, the FAA, Federal and local LEO's, and other emergency services.

Section 107.5 of the final rule outlines the duties and functions that the FAA expects the ASC to conduct in this regard. As the performance of those basic duties may vary in detail from airport to airport, the FAA does not anticipate issuance of an AC on this topic. However, the FAA will develop a suggested training curriculum, in coordination with the airport industry. The FAA expects that the training itself would not exceed 24 classroom hours, in most cases, and would average approximately 16 hours.

The FAA would expect the specifics of the training curriculum to be developed locally, in accordance with FAA guidance and local needs. The curriculum should and would be reflected in the security program.

Comments on § 107.5(c) Maintenance of Training Records: A commenter states that where ASC's training records are maintained is a matter of legal guidance and operational preference. As long as those records are available for FAA inspection upon request, there is no need for the FAA to micromanage record maintenance. The Port Authority of NY and NJ recommends removal of language specifying that records are to be maintained in the principal operations office.

Atlanta International Airport says that training records and other documentation requirements will create unnecessary recordkeeping burdens.

FAA response: The FAA has modified the rule so as to permit the airport operator to maintain the ASC training records in a location and manner of its choosing. Further, the FAA believes that the recordkeeping burdens would amount to no more than 30 minutes a year to document the training of each ASC. The FAA anticipates that a simple statement to the record that the ASC has completed training, as specified in the security program, with date and location, is acceptable. The FAA does not believe that this requirement is excessive.

Section 107.7 Inspection Authority

The FAA proposed to move existing § 107.7, ''Changed conditions affecting security'' to proposed Subpart B, § 107.107. In its place, the FAA proposed to insert § 107.7, ''Inspection authority,'' which included current § 107.27, ''Evidence of compliance.'' The proposed section would include the evidence of compliance requirements of existing § 107.27 and additional requirements based on the FAA's statutory authority to conduct inspections, investigations, and tests.

The FAA proposed that § 107.7(a) state the Administrator's authority to conduct inspections and investigations necessary to determine compliance with part 107 and the security program.

The FAA proposed that § 107.7(b) restate the language of existing § 107.27. Also, it was proposed that § 107.7(c) clarify the airport operator's obligation to provide FAA special agents the necessary access and identification media to conduct inspections. Significantly, this proposed requirement did not propose to require airport operators to provide access or identification media to any FAA employee other than special agents.

Comments on § 107.7(a): Miami International Airport suggests referring to special agents as FAA ''Security'' Special Agents.

Atlanta International Airport, Alaska Airlines, and Missoula International Airport state that § 107.7(a)(3) should be removed and placed in part 108 as it relates to carriage of hazardous materials by aircraft operators. Another commenter believes part 139 adequately addresses hazardous materials on airports.

The RAA, UPS, ACI–NA, AAAE, the Port Authority of NY and NJ, Detroit Metropolitan Airport, Lincoln Airport Authority, Federal Express, Phoenix Aviation Department, Tampa International Airport, and Denver International Airport had concerns regarding the FAA's inspection authority. These commenters state that the phrase ''at any time and place'' is too broad and could subject aircraft operators to unreasonable and frequent intrusions into all aspects of operations by untrained FAA personnel. These commenters, including Atlanta International Airport, recommend adding the word ''reasonable'' at the beginning of the phrase. One commenter states that this section should be amended to limit access by FAA special agents to only those portions related to their duties. Another commenter says that FAA special agents should be allowed to access airport operational areas only after they have received appropriate local training to ensure that safety is not compromised (such as, local rules, vehicle markings, driver's training). The ATA suggests that the FAA modify § 107.7(a) and (c) to state that the FAA provide written notice of an inspection to the airport operator 24 hours prior to commencing it. Atlanta International Airport requests that the FAA inspector be required to inform the airport operator or ASC of the inspection results.

FAA response: In response to the suggestion that the FAA refer to special agents as FAA ''security'' special agents, the agency notes that ''special agent'' is the correct term, and that ''security special agent'' is not a job title used in FAA service.

By statute, the Administrator is empowered to conduct inspections, investigations, tests, and other such duties as may be necessary to ensure the safety and security of the civil aviation system. Since performance of such inspections is not limited to special agents, it is conceivable that other FAA employees, from time to time, may be called upon to assist special agents in the performance of their duties on behalf of the Administrator. Therefore, to avoid confusion, the reference to special agents has been removed from § 107.7(a).

The FAA agrees with the commenters that hazardous materials inspections should be removed from part 107, however, it should not be placed in part 108. The FAA continues to have authority to inspect for violations of hazardous materials regulations, but its authority is based on different statute provisions than those for civil aviation security. Proposed § 107.7(a)(3) referred to determining compliance with 49 CFR part 172, which provides requirements under the Hazardous Materials Transportation Act. This reference has been removed from the final rule. Part 107 is devoted to civil aviation security issues. To avoid misunderstanding, reference to hazardous materials inspections is deleted.

With respect to concerns about the FAA's inspection authority, the Administrator is empowered to conduct such investigations and inspections as necessary to ensure the safety of civil aviation, under the statute. The statute, Title 49 USC Section 40113, does not restrict such activities by time and place, nor should they be restricted if the mission of the FAA is to be accomplished as effectively and efficiently as possible, and in the best interest of the public. Therefore, the FAA will not restrict its security-related activities through the regulation as suggested.

The FAA agrees with the commenters that the FAA is required to conduct its investigations and tests in a reasonable manner, but does not believe that the words ''reasonable'' should be added to the regulation. The wording used is similar to that used in a number of other FAA rules that have existed for years, including § § 119.59 (air carriers and commercial operators), 141.21 (pilot schools), 145.23 (repair stations), and 147.43 (aviation maintenance technician schools). The wording of these rules has not caused significant problems in the past. The FAA does not anticipate any change in its inspection procedures based on this new rule.

The FAA does not agree with the commenters who suggest that the access by special agents be limited in any way. The FAA has authority to conduct inspections and investigations throughout the airport property, wherever regulated activity is conducted. Any limitations placed upon FAA personnel acting on behalf of the Administrator could potentially hinder their ability to most effectively perform their assigned duties. Therefore, the final rule will not impose such limits.

As to the suggestion that the FAA provide advance notice of inspections, the FAA routinely notifies airport operators of scheduled inspections. This notice gives the parties to be inspected the opportunity to gather evidence of compliance and to arrange to have appropriate personnel available to assist the FAA. However, inspections related to a particular incident, or which are intended to be made without notice are necessary. Some inspections can only be effective if they are unannounced. Such considerations fall within the purview of the FAA's internal guidance and will not be addressed in this final rule.

Section 107.7(a) only provides for inspection by the FAA. Unlike the Notice, it does not refer to inspection by other Federal government entities. The FAA has no authority to grant or to deny inspection authority to another agency. The section was changed to avoid any appearance that the FAA was purporting to grant such authority.

Comments on § 107.7(b): Tucson Airport requests guidance to foster consistency when providing ''evidence of compliance with this part and its security program'' as described in § 107.7(b).

FAA response: Since its adoption, this provision has been intended to require airport operators to provide the FAA access to existing records. *See* 56 FR 41412 at 41416 (August 20, 1991). Such records may vary from airport to airport, and are not the subject of standard guidance.

Proposed § 107.5(a) referred to the Administrator making inspections and tests, and § 107.5(b) referred to the airport operator providing evidence of compliance to the Administrator. The final rule adds the clarification that these include the FAA making copies of records or the airport operator providing copies. Obtaining copies of records is an inherent part of the FAA inspecting compliance with safety and security requirements. It is necessary to preserve the records for further review by the FAA. This is true for all FAA inspections, including those by FAA aviation safety inspectors (who look at compliance with operational and airworthiness rules) and FAA special agents. Often, the copying is done at the aircraft operator's or airport operator's office with their permission. Sometimes other arrangements are made, such as the FAA temporarily removing the records to copy them at a FAA office or a commercial service. The FAA has rarely encountered difficulty on this point, but includes these explicit statements in the final rule to avoid misunderstanding in the future.

This section refers to copying of records, not just documents. Records may be kept in a number of forms, such as paper, microfilm, and electronic. The special agent may request copies of any of these forms, usually by having paper copies made of the records. If another form is easily used by the special agent, he/she may accept records in that form.

New § 107.7(c) states that FAA personnel may gain access to the SIDA and other controlled areas without holding access or personnel identification media issued by the airport or aircraft operator, when

necessary to conduct an inspection or investigation. The FAA agrees that in most circumstances FAA personnel should comply with the access and identification requirements in place at the airport, and it has been FAA practice to require that, when practicable, FAA personnel first obtain local media before conducting inspections. However, there are times when the FAA cannot adequately inspect and test compliance if its employees first obtain access and ID media from the airport or aircraft operator. The act of obtaining such media may provide an opportunity for the FAA representative to be recognized by personnel at the airport, thereby reducing or negating the value of the inspection. The FAA sometimes must make unannounced tests by entering the SIDA or other areas without first having obtained such media. The FAA authorizes such tests only under very controlled conditions, using personnel who are trained to avoid creating a safety hazard or an undue security response. For instance, they carry their FAA credentials to display if they are challenged, to immediately establish their authority to conduct such inspections. This technique is intended to be used only when it is not practicable to obtain local media before the inspection, such as when making unannounced tests of the access and identification systems in place. Otherwise, the FAA representatives have the appropriate access and ID media.

Comments on § 107.7(d): Atlanta International Airport states that proposed § 107.7(c) should be amended to delete the reference to ''any FAA special agent.'' The FAA should be required to designate a local point of contact to verify the need for local airport identification media. Commenters suggest it is difficult to maintain control and accountability of media issued to the FAA.

Juneau International Airport requests a description of valid FAA special agent credentials, as this information is currently not available.

The Port Authority of NY and NJ states that the display and wearing of an FAA special agent identification should be sufficient identification for unescorted access to any area of an airport which the agent has an operational inspection need.

The Sacramento County Department of Airports suggests that FAA special agents should have to go through the same identification media requests as an airport tenant. Ft. Wayne Airport suggests the FAA special agents should have to go through SIDA training to become familiar with the security program for which they are inspecting. Further, a commenter suggests the airports should charge reasonable fees associated with issuing airport identification media and providing SIDA training to FAA special agents.

Tucson Airport says that the Administrator should develop part 107 testing protocols that meet the FAA's needs without needlessly diverting resources to a ''cry of wolf.'' In a related comment, ALEAN states that it is unsafe for armed law enforcement officers (LEO's) to be running through airport terminals, believing that they are responding to an actual threat at the checkpoint when it is just a test. Such tests should be administered in the same manner that part 139 timed response drills are run.

FAA response: In response to the comment about deleting reference to ''any FAA special agent,'' the FAA agrees, in part, with Atlanta International Airport, and others that the proposed language was broad. Any FAA special agent seeking local access and identification media, should have an operational need for the media, and the concurrence of the designated local FAA point of contact. The proposed rule stated that the media would be issued on request of the FAA special agent and presentation of credentials. As some commenters note, not all FAA special agents have duties and training to conduct inspections at the airport, and those agents do not need local media. The Administrator (usually through the local FAA field office) will provide to the airport or aircraft operator the names of special agents who require media.

In response to the request of Juneau International Airport, the commenter is welcome to request and to view the FAA special agent credentials in the possession of any special agent. They may contact the local FAA security office to view those credentials.

In response to the comment by the Port Authority of New York and New Jersey about the display and wearing of special agent identification, the FAA has addressed that under the new § 107.7(c). When exercising such privileges it is anticipated that the FAA employee acting on behalf of the Administrator will be in the possession of, but not necessarily displaying such credentials, as the situation may warrant. The circumstances under which this authority could be exercised include surveillance and unannounced testing or inspections.

Regarding the comment by the Sacramento County Department of Airports, the FAA acknowledges that appropriate safety and security-related training should be provided to FAA special agents before they exercise full access privileges to the secured areas and AOA's of the airport under normal circumstances. The aspects of such training that have common application can be provided at the agent's primary duty location and can be supplemented with local training at other airports requiring such training. This approach is in common use today, throughout the industry for those persons requiring similar access privileges. The revised § 107.7(d) addresses these concerns. However, in emergency situations or other initiatives, the responding agents may not have been provided the training or access media for that particular airport. The exigencies of their duties may require this access media, therefore, the language of the final rule has been modified accordingly. Where appropriate, coordination through the ASC or other local authorities would take place.

In response to the comment about allowing the airport to charge reasonable fees for issuing airport identification media, the FAA notes that nothing in the regulations would preclude the airport operator from imposing reasonable charges for its services. In fact, many already charge for initial identification media and issuance of replacements. Consequently, language permitting the airport to do so is not necessary in the final rule.

Regarding the comment about developing part 107 testing protocols, the FAA appreciates the complexity and sensitivities of the regulated parties' ongoing operations. The agency also understands both the importance and the impacts of its own operations, especially while conducting essential testing. These testing efforts will continue under the FAA's internal guidance. The agency will continue to be mindful of actual safety and security concerns during testing operations and will maintain dialog on this subject with the industry at the local and national levels.

The final rule states that the media must be issued ''promptly.'' The FAA expects that the media will be issued without undue delay, generally within a similar time frame that media are issued to airport, aircraft operator, and contractor employees who need the media. The particular procedures will be worked out at each airport with its FAA field office.

In response to ALEAN's comment, the FAA understands and concurs with the proposition that safety in testing is essential. The FAA also believes that testing of a law enforcement response differs in some aspects from testing

firefighting and other emergency responses. For example, the latter services tend to be more focused on a more specific range of duties and generally operate from a fixed position. Law enforcement response is a resource with numerous missions unrelated to civil aviation security as addressed in this rule, and which can take it away from the immediate vicinity of the passenger screening facilities. As such, the law enforcement response can originate from anywhere, but must arrive at a designated location within a given timeframe. The FAA recognizes that testing of the law enforcement response must be conducted as judiciously and as safely as possible. Often, that can be accomplished with full disclosure in advance to the law enforcement agency. The FAA will continue to share ALEAN's concerns with its special agents but does not believe it appropriate to modify any portion of part 107 in this regard. Instead, such concerns will be addressed through the FAA's internal guidance and in keeping with the missions of both the law enforcement entities involved, the airport operators, and the FAA.

Section 107.9 Falsification

The FAA proposed a new § 107.9, entitled ''Falsification.'' This section is the same as the current § 107.2 adopted on November 27, 1996 (61 FR 64242, December 3, 1996).

Comments: The UPS and Atlanta International Airport request an outline of the enforcement procedures and guidance to the airport operators for falsification findings. The commenters say that the airport operator should be informed of all investigations and be provided a copy of the report of findings.

The UPS, Port Authority of NY and NJ, Detroit Metropolitan Airport, and Lincoln Airport Authority say that it should be stated that persons are directly accountable to the FAA for compliance with this regulation, including federal enforcement procedures and fines.

FAA response: Enforcement procedures are contained in 14 CFR part 13 and in FAA order 2150.3A. There is no need to repeat the procedures in part 107.

Section 107.11 Security Responsibilities of Employees and Other Persons

In this section, the FAA proposed to prohibit persons, as defined in part 1, from tampering or interfering with, compromising, or modifying any security system, or attempting to do so. It also proposed to prohibit carrying a deadly or dangerous weapon, explosive, or destructive substance into sterile areas, critical security areas, or restricted operations areas.

This section proposed the use of civil penalty actions to penalize persons, those employed by the airport operator and those not under the direct authority of the airport operator (such as trespassers), who fail to comply with this section.

The FAA proposed in § 107.11(c), that individuals authorized by the Federal government, airport operator, and aircraft operators would be allowed to conduct tests and inspections of security systems.

The FAA proposed in § 107.11(d) that provisions of this section that apply to firearms and weapons would not be applicable to law enforcement personnel, Federal Air Marshals, and certain individuals authorized in a security program to carry a weapon.

Comments on § 107.11(a): Atlanta International Airport and Roanoke Regional Airport request an outline of the enforcement procedures and guidance to the airport operators for noncompliance by individuals. The enforcement concept requires more explanation. The airport operator should be informed of all investigations and be provided a copy of the report of findings.

Port Authority of NY and NJ is concerned that the majority of enforcement of Federal responsibilities are placed on the airport. The Port Authority holds that the FAA should not be unique among Federal enforcement and oversight agencies in abdicating its enforcement responsibilities.

Burbank Airport Authority suggests that civil penalties should be up to $10,000 on a case by case basis, rather than $1,000 as stated in the preamble.

The UPS, RAA, Federal Express, a local department of aviation, Miami International Airport, and many other commenters support the adoption of proposed regulations which would require individual accountability to the FAA and use of civil penalties and enforcement actions against employees, contractors, and other individuals.

The ACI–NA, AAAE, and an airport suggest language stating that failure to comply by an individual will result in revocation of privileges, application of fines, or other punitive action by the Administrator. They also suggest language stating that this rule would not prohibit State or local governments from adopting similar or more stringent regulations for local enforcement. On the other hand, ALEAN suggests that the NPRM is a superficial and impractical attempt to solve a lack of personal accountability and responsibility.

FAA response: The enforcement procedures are found in part 13, Investigative and Enforcement Procedures, and FAA Order 2150.3, Compliance and Enforcement Program.

In further response to ACI–NA and AAAE, the FAA does not believe there is a need for the agency to insert language stating that the rule would not prohibit State or local governments from adopting similar or more stringent regulations. Many State and local governments are currently permitted to adopt similar or more stringent security rules within the context of their respective jurisdictions. Many have already done so. Airport operators are primarily responsible for the security and safety of their airports, both for civil aviation security and other security issues they encounter. As part of this effort, they adopt rules and procedures to gain compliance of their employees, contractors, tenants, and others with safety and security rules. Absent very unusual circumstances, State or local governments are free to adopt penalty provisions to promote compliance.

In response to UPS and other supporting comments on individual accountability, the agency wishes to emphasize an increased reliance on individual accountability, particularly with regard to a person's interaction with security measures. But, at the same time, the agency also emphasizes that the airport operator and aircraft operator are responsible for ensuring that their employees, contractors, and others comply with security duties. The FAA agrees with ALEAN that this section is not, standing alone, adequate to address all issues of individual compliance with security rules. It is intended to serve as another tool to assist the airport operators, aircraft operators, and others to emphasize the responsibility of individuals and other persons to do their part.

Proposed § 107.11 outlined provisions of the regulation for which individual accountability would attach. However, aside from the merits of this proposal, much attention, as reflected by the comments, seemed to focus not on § 107.11, so much as on the related impact of proposed § 107.103(a)(2). This language would have required the airport operators to establish and carry out an enforcement program to hold persons in violation of the program accountable at the local level. As discussed above, the comment period was reopened for that provision.

Burbank Airport Authority sought an increase in the amount of civil

penalties. The maximum civil penalty is set by statute, however, as to individuals in these circumstances, the amount is $1,100 (adjusted for inflation since Notice 97–13 was issued).

The FAA notes that the circumstances surrounding a single security violation may involve more than one responsible party. For example, if an employee circumvents an access control to a secured area, and gains unauthorized access to an aircraft, that person can be held individually responsible for his/her actions under new § 107.11(a). At the same time, the airport operator may be responsible for failure to control access to the secured area under new § 107.201(b), and the aircraft operator may be responsible under part 108.

This rule will also have the effect of prohibiting some unauthorized testing if it violates § 107.11. The unauthorized testing of security systems may be a form of compromise, circumvention, or interference. An example is a person who is not authorized to be in the secured area without escort, but who deliberately enters the secured area without escort. Many of these actions may serve to distract unnecessarily security or law enforcement resources from their duties, increasing the risks from actual threats. Such unauthorized ''testing'' of security systems can prove dangerous to the ''tester'' (such as if they are not aware of the safety issues in the AOA, with taxiing aircraft and other hazards). The final rule language is consistent with this position, and can be cited in holding accountable persons who conduct such unauthorized activities.

Comments on proposed § 107.11(b): Anchorage International Airport states that § 107.11(b) seems appropriate for what is now known as the ''sterile area'' or ''secured areas'' of the airport, not for areas that are currently known as the ''restricted areas.''

Miami International Airport and TWA state that § 107.11(b) should clarify that compliance with this section rests on the individual and not the airport.

Roanoke Regional Airport states that § 107.11(b) does not recognize that construction contractors may need to bring explosives into secure areas of the airport.

The Port Authority of NY and NJ, Northwest Airlines, and Detroit Metropolitan Airport question the means by which the airport can ensure that no person will have ''any deadly or dangerous weapon, etc.'' without screening all employees. Several commenters request clarification of ''deadly or dangerous weapon'' and ''other destructive substances.''

The ATA, UPS, and Federal Express strongly object to the imposition of screening procedures for employees at access points controlled by proposed § 107.205, and to rescreening of employees who have access clearance from the airport to enter secured areas.

FAA response: In the proposal, the agency sought to provide a means by which unauthorized persons carrying deadly or dangerous weapons, explosives, or incendiaries into the secured area could be held liable under the agency's compliance and enforcement program. The proposed language provided for persons who would have to carry such items into the secured area in the course of their authorized duties. After careful review, the agency has determined that local airport operators, through their local rules and laws, and law enforcement personnel, have the responsibility, authority and the capability to control the presence of weapons and other deadly items on airport property. Hence, there does not appear to be a need to introduce any new rulemaking regarding this issue at this time. The FAA has decided not to adopt proposed § 107.11(b), as well as the related language under § 107.11(c). Over time, the agency will monitor any incidents relating to persons carrying unauthorized weapons or deadly or dangerous items that may be detrimental to the flying public and if warranted, will develop comprehensive security measures.

Section 107.101 General Requirements

The FAA proposed this new section to incorporate related provisions of the existing regulation that require the security program to be current and in writing, and that a copy be kept at the principal operations office. The program's objective was proposed to be modified to include protection against the introduction of a deadly or dangerous weapon, explosive, or incendiary onto aircraft.

In the preamble, the FAA noted its intention to develop a standard airport security program, similar to the air carrier standard security program.

Comments: The ATA and Tucson Airport request that if the use of a standard airport security program is to be a mandatory requirement, then the airports should be given an opportunity to review and comment on its contents and application effects, prior to implementation. The additional time would provide consistency of airport and aircraft operator security programs and benefit the passengers, baggage, and cargo processing. Any policy directives for the model program should also be made available for review and comment.

FAA response: Upon review, the FAA has determined that it will be easier, less disruptive, less expensive, and equally effective to not develop a standard security program, but to modify the language of § 107.101(a)(4) to require that airport security programs include an index, arranged according to the order of subject areas cited in § 107.103. This requirement will preclude the need for major security program modifications. The FAA is also convinced that an index in each security program, arranged in accordance with this standard format, will moderate significantly the FAA's difficulties associated with overseeing the hundreds of vastly different security programs across the nation. The final language has been modified to that end.

Comments on § 107.101(a): Atlanta International Airport states that proposed § 107.101(a) should be written to reflect that airports are responsible for the safety and security of persons and property while at the airport. Roanoke Regional Airport states that the aircraft operator must be responsible for the security of persons and property onboard the aircraft.

Continental Airlines requests that § 107.101(a)(1) be clarified to exempt passenger checkpoint screening responsibilities from the security programs.

FAA response: The FAA believes that the delineation of authorities, for example the screening of passengers or the provision of law enforcement response, are properly assigned based on statute, regulation, reasonable attachment of liability, and the authority possessing the appropriate resources. The term ''on an aircraft operating in air transportation in air commerce'' reflects that the mandated measures in the statute at airports are ultimately in support of the security of person on board aircraft, and are not designed to address other security concerns. The proposed language was included because some of the airport's tasks do include support of the screening function, which prevents the introduction of weapons, explosives, and incendiaries on an aircraft.

Federal law assigns solely to aircraft operators the responsibility for passenger screening. That law cannot be overcome by regulation. Rather the intent of § 107.101(a)(1) is to emphasize the airport operator's role in supporting the screening system in cooperation with aircraft operators.

Comments on § 107.101(b): Atlanta International Airport, Tucson Airport, Minneapolis Airport, Port Authority of

NY and NJ, Detroit Metropolitan Airport, and Lincoln Airport Authority state that the ''principal operations office'' may not be the appropriate area to store the security program. Denver International Airport believes that specifying the storage location of the security program is not necessary and that making the security program available to the FAA for review upon request should be sufficient. However, requests from the FAA to review the security program should be made through the ASC.

FAA response: Upon reflection, the FAA agrees with the commenters. The rule language has been modified to delete reference to the ''principal operations office.'' Instead, the airport operator is required to maintain at least one current and complete copy at the airport and to provide a copy of the security program to the Administrator upon request. In most cases, the ASC required under new § 107.5 would be the primary contact for such requests.

Section 107.103 Content

The FAA proposed this new section to describe the required content of the security program. The proposed rule specifies three different levels of security programs varying in complexity. The most comprehensive security program would continue to be applicable to airports serviced by scheduled passenger operations on aircraft with more than 60 seats.

The type of passenger operations that trigger the two remaining types of security programs have been expanded somewhat, as the result of changes to part 108. The intent is to ensure complete protection of the sterile area and to ensure security of passengers.

Comments on proposed § 107.103(a)(1): Atlanta International Airport, Missoula International Airport, and Phoenix Aviation Department request removal of the requirement to outline the ASC's training. Training requirements should be provided in an advisory circular (AC), not the security program.

Juneau International Airport requested the FAA explain what the training requirements for ASC's and alternates are under § 107.103(a)(1).

FAA response: While ASC training has been addressed in the discussion of § 107.5, it seems appropriate to address the administrative aspect of the ASC training program requirements here. The FAA disagrees with comments submitted by the Atlanta, Missoula, and Phoenix airport authorities that the ASC training requirements should appear in AC's. Rather, the agency believes general training mandates appearing in the regulation must be clearly defined and required under specific language appearing in nonpublic security programs. The agency notes that the guidance in AC's is not mandatory. The proposed language is adopted without change.

Comments on § 107.103(a)(2): Numerous comments were received on the proposal to require each airport to have a security compliance program.

FAA response: As explained above under General Discussion of the Rule, the comment period on this section was reopened. The FAA will respond to all comments in a later action. The comments recounted here are only a representative sampling of the many comments received in response to proposed § 107.103(a)(2). Yet, since the close of the comment period, the FAA has become aware of shifting views by many of the same parties with regard to this and related issues. Therefore, the FAA has reserved decision on proposed § 107.103(a)(2), and reopened the docket for comments on August 10, 1999. The new comment period closed on September 24, 1999. The FAA will consider the comments received and consider what action, if any should be taken on this proposal.

Comments on § 107.103(a)(3)–(20): Five airports suggest that the FAA replace the word ''dimensions'' in § 107.103(a)(3)(i) with ''general description.'' A general description or a map would provide sufficient details of the areas. Information about the dimensions of the map should be delegated to appendices and not subject to FAA approval. Ft. Wayne Airport says that a scale map or diagram has been and should be sufficient to delineate these areas. If the FAA needs more detailed information, it should state the reason behind the requirement and include costs associated with calculating the dimensions of these areas into a cost benefit scenario. Quad City International Airport states that detailed map-making is a costly undertaking.

Denver International Airport and Port Authority of NY and NJ recommend modifying § 107.103(a)(5) to state ''sterile areas with direct access to the critical security area.'' Only those activities with direct access to secured areas in the NPRM from the sterile areas should be listed.

Another commenter recommends deleting any references to ''sterile areas'' in proposed § 107.103(a)(5) and throughout part 107 since the term is not defined.

Tucson Airport states that the following information should be outlined in an appendix, not included in the body of the security program: The system for maintaining records and the schedule for reporting them required by proposed § 107.103(a)(12), the contingency plan required by proposed § 107.103(a)(14), the exclusive area agreements required by proposed 107.103(a)(19) and the tenant security agreements required by proposed § 107.103(a)(20).

One commenter states that the incident and emergency management procedures, required by § 107.103(a)(17) are adequately covered for airports complying with part 139 programs. A reiteration of these procedures would be redundant and a cross-reference to the part 139 emergency plan should be sufficient.

FAA response: The FAA disagrees with the commenters that a ''general description'' rather than ''dimensions'' would suffice in describing various aspects of the airport in the security program. The FAA believes that the exact dimensions and boundaries, as required in the security program, are necessary to clearly establish where various security measures are required at different locations on the airport. With the advent of the tenant security program (new § 107.113), and the possible increased reliance upon exclusive area agreements (new § 107.111), this requirement becomes increasingly important. The detailed descriptions are necessary so that all parties are aware of what security procedures apply in what areas, and which party is responsible for carrying out those procedures. At the same time, the FAA does not expect the airport operators to generate detailed maps drawn specifically for this purpose. Rather, existing maps used for engineering and maintenance at most airports are usually acceptable and are in common use today. The wording remains the same. If an airport has a method of clearly identifying the boundaries of the areas without using dimensions, it may request to use that method.

In considering the comments that stated that only sterile areas leading to critical security areas (now secured area) should be detailed, the FAA notes that while most sterile areas have access points leading directly to secured areas, that condition may not be the case universally. Further, there are other considerations besides access to secured areas that forces the FAA to require that such details appear in the security program. Lastly, the FAA does not accept the suggestion to delete the term ''sterile area,'' since it is not defined in this part. It is defined in the final rule

to part 108, in § 108.3, and is a commonly used and understood term.

A security program may be structured in the manner suggested by the Tucson Airport by incorporating information appearing in program appendices. New § 107.103(d) (and current § 107.3(c)) provides for including information in an appendix.

As to the comments regarding proposed § 107.103(a)(17) regarding incident management (new § 107.103(a)(18)), the FAA wishes to emphasize that the requirement speaks to the evaluation of a threat, rather than to a response to an actual incident as referenced in § 139.325. The level of response to a threat is tied to the evaluation of that threat, which is a different process than responding to an actual highjacking or other event in progress. Evaluating which threats call for what type of response is a security issue, best handled under part 107. It may involve evaluation of non-public security information.

Comments on § 107.103(b) and (c): Minneapolis Metropolitan Airport states that the procedures for public advisories required by § § 107.103(b)(7) and 107.103(c)(6) (i.e., that a foreign airport has, in the judgment of the Secretary of Transportation, failed to maintain and administer effective security measures (new § 107.305)) should rest with the aircraft operators, that should be responsible for informing their passengers. This should not be an airport operator responsibility.

FAA response: The requirement to provide public notification that a foreign airport has been determined to have failed to maintain or carryout effective security measures, is found in the Section 44907(d)(ii), Title 49, United States Code. The FAA believes the requirement to prominently post the identity of such foreign airports at all U.S. airports having regularly scheduled aircraft operator operations is best accomplished at each U.S. airport by a single entity at each location. For consistency's sake, the FAA has determined that the airport operator should be responsible for the posting of this information. The law also requires aircraft operators serving the subject airports to notify their passengers of the foreign airport's status. With this dual requirement, the FAA believes all persons using the airport, and those using the specified carriers, will have ample warning before risking travel to a location that the Secretary of Transportation has determined lacks effective security measures.

Comments on § 107.103(d): Tucson Airport asks whether the FAA would allow inclusion of an airport's part 139 emergency plan in the appendix as sufficient compliance with this rule.

FAA response: Regarding placement of the part 139 emergency plan in the security plan as an appendix, the FAA notes its previous comments, above. It has no objections to this method where the plans are mutually supportive and meet the requirements of the respective parts. However, the FAA's civil aviation security organization's review and approval process of the security plan may employ different criteria than the reviews under part 139, for the review of the emergency plan. Simple inclusion in the security plan without the opportunity for the FAA's civil aviation security organization's review and approval on a case-by-case basis would not be acceptable. Additionally, only those limited portions of the emergency plan with direct relevance to security concerns should be incorporated into the airport security plan.

Section 107.105 Approval and Amendments

The FAA proposed to combine existing § § 107.5, 107.9, and 107.11 into a new section, proposed § 107.105. Several changes were proposed to the amendment process itself. Proposed § 108.105 prescribed the same approval and amendment procedures for aircraft operators.

Throughout this proposed section, any references to the ''Director of Civil Aviation Security'' were replaced with ''Assistant Administrator.'' Also, time restraints on filing petitions for reconsideration of the FAA's decision were included for airport operators. Specifically, § 107.105(a)(2) proposed that airport operators submit to the Administrator a petition for reconsideration within 30 days after receiving the notice to modify. Proposed § 107.105(a)(2) included the provision in current § 107.11(c) that the filing of a petition would stay the notice to modify pending a decision by the Administrator. Section 107.105(a)(3) proposed that the Administrator disposes of any petition within 30 days of receipt.

Section 107.105(b) prescribed procedures for an airport operator to request an amendment to its security program currently covered under existing § 107.9. The FAA proposed to increase the number of days prior to the effective date that the airport must submit its proposed amendment from 30 to 45 days. The proposed rule also noted that the amendment process may take longer than 45 days if the proposed amendment was modified or denied.

Existing § 107.9(b) states that the FAA will respond to an amendment proposed by the airport operator within 15 days. The proposal extended this time period to give the FAA 30 days after receipt for approval or denial of the proposed amendment.

In proposed § 107.105(b)(4), the FAA proposed to modify existing § 107.9(d) to limit the time that an airport operator may petition the Administrator to reconsider the denial to 30 days.

Retention of the FAA's existing procedures to amend a security program was proposed in § 107.105(c) and (d). Two significant changes, however, were proposed to the existing procedures of § 107.11: (1) A new requirement for airport operators to submit petitions for reconsideration no later than 15 days before the effective date of the amendment, and (2) a clarification that a petition for reconsideration stays the effective date of the amendment, unless the emergency procedures are used.

Comments: Miami Airport states that there must be procedures in place to ensure that amendments are not sent into an abyss which is created by returning the amendments to airports repeatedly for rewrites, or with general disapproval language that does nothing to aid the airport to satisfy the FAA's objective. Another commenter states that as written, this section leaves the airport with the feeling that there will be even longer delays to requests from airport for items that are essential to airport operations.

FAA response: The FAA agrees with the proposition that amendments, when submitted by airport operators, must be handled in a timely manner and in good faith. They must be submitted in the same manner. In practice, the complexity of any given amendment and the differences between the respective positions of the FAA and the airport operator will determine how often the amendment is handled and how long the process will take. The regulatory language appearing in the final rule attempts to place good faith constraints upon the parties, but recognizes that the exigencies of business as well as other factors often preclude strict adherence to deadlines. It is, therefore, in the mutual interest of both the operator and the FAA to work closely to agree upon amendment language that has been submitted as completely and in the most timely manner possible.

Comments on § 107.105(b): Several commenters suggest that this section should be amended to require the FAA to acknowledge receipt of an airport's proposed amendment within 5 business days. Within 30 days of receipt, the FAA should either approve or deny, in writing, the proposed amendment. One

commenter had submitted a proposed amendment to the FAA with no action for 11 months.

One commenter states that the submission of amendments to the Administrator presents problems, since airports dissatisfied with local FAA replies, could submit their requests to Washington.

Another commenter suggests that the FAA's civil aviation security field units (CASFU) should be required to review and return comments to airports within 120 days after receipt of an airport-submitted security program amendment. The FAA personnel should be required to approve and return the final security program to the airport for initiation and distribution to the necessary parties, within 60 days after any required resubmission by the airport of the final version of the security program.

The ATA and Anchorage International Airport oppose increasing the time for the FAA to approve an amendment request for either an airport operator or an aircraft operator and recommend that the FAA expedite the amendment process.

The ACI–NA and AAAE oppose the changes to the amendment procedures that impose more stringent deadlines on the regulated parties and relax the time burden on the FAA. These commenters recommend a modification to the rule that would require the airport to submit the amendment 30 days prior to the proposed effective date. Then, the FAA would have 15 days after receipt to approve, deny, or question the amendment, after which the airport operator would have 15 days to respond to the FAA's request.

FAA response: The FAA agrees that the airport operator is entitled to an acknowledgement of receipt of a proposed amendment. The FAA does not believe that this issue needs to be resolved through the regulation, since the airport operator can have the amendments hand-delivered, or sent via return receipt mail.

Also, the agency has noted elsewhere that references to the Administrator are to be interpreted as referring not only to that office, but to a subordinate level of the civil aviation security chain-of-command. This level would include the Assistant Administrator and the subordinates to whom he has delegated program authority, as noted in § 107.1(b).

As noted above, the FAA concurs that the expeditious handling of amendments is essential, and that every effort is made to ensure their timeliness. The agency will strive to meet that commitment.

The agency has carefully considered the time constraints the regulation will place upon all parties to the amendment and the approval process. The FAA has decided to implement a timeframe that it believes is fair and equitable when approached by all parties in good faith. It should also be noted that, in practice, the regulated parties have often requested amendments for activities that were to take place much sooner than the regular amendment process call for. The FAA often handles these on an expedited basis.

The FAA also notes that exclusive area agreements under § 107.111(b) and tenant security programs under § 107.113(a) may be terminated at any time by the FAA if it is determined to be in the interest of security and safety.

Comments on § 107.105(d): Miami International Airport, Lincoln Airport Authority, Federal Express, and Denver International Airport support the ASAC recommendations that Emergency Amendments be issued to the airport program with expiration dates.

Tucson Airport and Port Authority of NY and NJ state that FAA Emergency Amendments should be ''sunsetted'' 180 days from date of issuance if not canceled sooner. The 180-day constraint would not preclude reissuing of the Emergency Amendment, but would build in a review of the propriety and effectiveness of measures to be implemented.

One commenter states that there should be some provision to allow for local modifications to the FAA amendments.

Sacramento Department of Airports states that the current practice of policy memoranda should be discontinued. While there are instances where changes must be issued immediately, in memoranda, these memoranda should be followed up by the FAA within 30 days from the official regulatory change.

FAA response: The comments received in response to this section dealing with ''Emergency Amendments'' illustrate the different practices that have developed. In its original context, ''Emergency Amendment'' was used for exigent and permanent change to the basic individual airport's security program. It also has been used much like the Security Directive process available for several years to aircraft operators under § 108.18, that is, an amendment issued to address time critical threats that are expected to have a limited duration. Depending on the nature of the threat upon which the Emergency Amendment was based and the measures imposed, an expiration date was either set or left ''indefinite.'' But, in either case, the directive nature of the Emergency Amendment was focused on a specific threat, ostensibly with a finite period of applicability.

The final language of this section is intended to return this process to one in which permanent changes to the actual security program are made based upon such emergencies as may arise. Response to certain threats of finite duration, that were formerly handled by Emergency Amendments, now may be addressed in the new § 107.303, Security Directives and Information Circulars. The agency now intends for Emergency Amendments to security programs to be used for exigent changes made to the individual security program, on what is expected to be a permanent basis.

The FAA wishes to assure the regulated parties that it does not issue security program changes through policy memoranda. While memoranda are used for the FAA's internal guidance regarding ongoing programs and enforcement policies for existing requirements, the Emergency Amendment process under § 107.105(d) will only transmit Emergency Amendments to airport operators under cover memoranda. In many cases, where temporary emergency measures subsequently have become part of the baseline, those changes have been proposed through the normal process, with comments invited and considered before any final determination had been made. The FAA has become increasingly sensitive to the airport operators' concerns in this regard, and will continue to follow that practice under the new § 107.105, and as will be noted later, § 107.303.

Section 107.107 Changed Conditions Affecting Security

Proposed § 107.107 would expand the types of changed conditions that would require operators to take corrective actions. It would expand the scope of the requirement to encompass all the elements of the security program to ensure that any changes that may impact security would be reported to and addressed by the FAA as soon as possible.

As proposed, the airport operator would be required to report any changes in the physical layout of the airport, both areas relating to airport operations and aircraft operator operations. The proposal would augment the existing procedures for the airport operators to follow when a changed condition occurs by requiring the airport operator to initially notify the FAA within 2 hours, or within an approved timeframe, of the discovery of any changed condition that

could affect how an airport complies with regulatory requirements.

The proposal would require the airport operator during this initial notification to obtain verbal approval of any interim measures to be taken to maintain adequate security. The proposal would continue to allow the FAA to issue emergency security program amendments under proposed § 107.105(d) if an agreement on adequate interim measures could not be reached. However, the proposal provided relief in responding to short-term changes.

Proposed § 107.107(c) and (d) would require the airport operator to follow certain procedures to amend its security program to reflect the change. For changed conditions under 60 days' duration, § 107.107(c) proposed that the airport operator be relieved from the amendment process required under proposed § 107.105 and only be required to provide written notification within 72 hours for FAA approval. Recognizing that many changed conditions affecting security can be readily resolved in less time than it would take to complete the formal amendment process, the FAA sought this change to provide some relief in reporting short-term or temporary changes while ensuring that the FAA retains oversight of temporary or short-term changed conditions to security.

Proposed § 107.107(d) would provide procedures for the disposition of changed conditions anticipated to be over 60 days in duration.

Comments on § 107.107(a): Atlanta International Airport, among others, stated that the airport operator cannot be held accountable to notify the FAA of changes of aircraft operator operations, level of services, and aircraft. Miami International Airport and Ft. Wayne Airport state that this requirement would be more appropriate in parts 108 and 129.

The CALA states that changes should only include things as airport perimeter and structural redesigns, relocation of screening checkpoints, and redefining of airport secured areas. Miami International Airport, Port Authority of NY and NJ, and Lincoln Airport Authority state that the layout and physical structure (§ 107.107(a)(3)) can change frequently during construction. An overall construction plan should be submitted to the FAA, but not a constant series of notifications about the changes.

The ATA requests very clear criteria as to what ''changed conditions'' are, to satisfy the notification requirement. Denver International Airport suggests that ''changed conditions'' should be limited to conditions that have a serious and continuing impact on security. Furthermore, it was stated, the FAA did not consider the cost associated with personnel staff changes and equipment requirements for scheduling notification to comply with the newly revised notification requirements.

FAA response: In response to these comments, the FAA would like to clarify that its intent is that the only changes which need to be reported are those that cause the airports to be out of compliance with the provisions of part 107 or the FAA-approved security program, at the time the changed condition occurs. Furthermore, this section is not intended to include all construction projects, only those that impact its security program, such as access, movement control functions, and its support of passenger screening checkpoints. The language of the final rule has been modified to more accurately reflect that position, and to provide greater latitude to the airport operator insofar as the required timeframes for reporting changes that impact its compliance posture.

Comments on proposed § 107.107(b): Thirty-four airports, two local governments, a State government, six local departments and commissions of aviation, two airlines, and UPS suggest that a 2 hour initial notification of changed conditions is unnecessary and an arbitrary timeframe. These commenters state that the FAA does not seem prepared to handle the information overload for after-hours, weekend, and holiday occurrences when it is anticipated that FAA field reps would not be available to receive such information. These commenters recommend that the requirement to verbally contact the FAA should apply only to changes that seriously impact security and only as soon as practicable (such as within 24 hours of discovery by the airport operator). The option to provide this information electronically should be considered (such as e-mail and fax). On the other hand, ACI–NA and AAAE recommend that notification should occur within 48 hours. ATA suggests deleting this section because it lacks clear definition.

FAA response: The FAA agrees that a 2-hour initial notification of changed conditions may not be an acceptable timeframe. To provide some flexibility to the operators, this section has been modified to provide that notification be made within 6 hours of discovery or other timeframe for notification to be established in the individual security program. Further, while FAA field offices are not open 24 hours a day, telephone notification can be made to alternate contact numbers for field office staff.

Section 107.109 Alternate Means of Compliance

The FAA proposed this new section to provide relief for small airports located in communities that are only served by seasonal air carrier operator or foreign aircraft operator traffic (such as ski resorts), remotely located, subject to extreme environmental conditions, or have limited facilities and few employees. Often these airports serve aircraft larger than 60 seats for only a portion of the year, or on an infrequent but regular basis. This section would permit the FAA to approve airport operators of such airports to use alternative means to comply with the requirements of the rule. To petition for relief from part 107 requirements, larger airport operators would still have to use the exemption process under existing § 11.25, Petitions for rule making or exemptions.

Comments: The FAA received some comments regarding unique alternate measures at specific airports.

FAA response: Alternate measures at specific airports must be considered case-by-case and questions regarding them cannot be resolved in this rulemaking.

Section 107.111 Exclusive Area Agreements

Proposal: The notice proposed that the Administrator may approve an amendment to an airport security program that permits an air carrier or foreign air carrier that has an approved security program under part 108 or part 129 to assume responsibility for specified security measures for all or portions of the critical security areas or restricted operations areas. The exclusive area agreement must be in writing and must include all of the necessary information, as indicated in the NPRM, to be considered complete.

Comments: A commenter recommends that regulated entities be held responsible for the activities of their unregulated contractors, permitees, invitees, etc. The ALPA and RAA comment that the FAA should allow exclusive area agreements to be developed, which create joint liability and responsibility for the airlines involved. The RAA notes that this requirement could take the form of a consortium to share responsibilities.

Roanoke Regional Airport states that if the airport is conducting the ''monitoring and auditing'' to ensure compliance, then no ''responsibility'' transfer has occurred and such an

''exclusive lease'' for that purpose would be meaningless.

The ACI–NA and AAAE propose new language stating that the FAA may unilaterally revoke the agreement and descriptions of punitive actions that may be imposed on the aircraft operator or its employees by the FAA for violations of security regulations.

The ATA believes that no security requirements other than those agreed to by the parties to the agreement should be mandated.

One airport asks if the carrier's leasehold agreement could serve as the binding document for exclusive areas. If not, specific guidance for exclusive area agreements should be provided in an AC.

The Port Authority of New York and New Jersey and the city of Phoenix request that the words ''or one entity'' be added to § 107.111(a) after the phrase ''foreign air carrier,'' to allow air carriers to form a consortium or a corporation, like fuel farms and other enterprises operating international terminals. Shared responsibility should be allowed, but only when there is a legal entity established as the responsible party to ensure that the FAA has the ability to enforce the regulations.

FAA response: The FAA agrees that regulated entities are responsible for the actions of their unregulated contractors. The regulation provides for this concern by not excluding the regulated entities from such responsibilities. Hence, the FAA does not believe it is necessary to modify the proposed language in order to respond to the comment. The fundamental responsibilities for compliance with this part rest with the airport operator or on an aircraft operator or foreign air carrier under an exclusive area agreement.

Under the existing exclusive area provisions of § 107.13, and new § 107.111, the FAA's intent is for the airport operator to maintain an awareness of the security posture of the area covered under the agreement. To avoid misunderstanding, we have not adopted proposed § 107.111(b)(4) and (5) regarding the airport monitoring and auditing the aircraft operator, or terminating the exclusive area agreement. The FAA expects the ASC to maintain a general awareness of all security functions, and raise with the aircraft operator and/or the FAA any apparent deficiencies.

The FAA will continue to be responsible for inspection duties in exclusive areas, and for ensuring compliance, and will initiate enforcement actions when necessary.

The FAA agrees with the suggestion made by ACI–NA and AAAE that the regulation permits the agency, in extraordinary circumstances, to unilaterally and immediately terminate exclusive area agreements. In most cases the FAA will work directly with the aircraft operator to correct the problems. However, since poorly implemented agreements represent a vulnerability in the system, and thereby compromise the safety of the larger community, the FAA sees a clear connection between such circumstances and the need for immediate termination, and the return of the responsibility to the airport operator. For that reason, the procedures set forth in § 107.105(d), Emergency Amendments, would be employed for that purpose. The FAA sees no need for additional language toward that end in this section.

On the issue of joint liability and responsibility, the FAA has chosen not to provide such latitude. The agency believes that when more than one party holds joint responsibility for such matters, the responsibilities often are overlooked under the presumption that the ''other'' party will act. In that same view, a shared agreement might tend to fragment responsibility. Not that this would not prevent several aircraft operators from using the same portion of the secured area. Only one of them, however, could have an exclusive area agreement for a given part of the secured area.

The proposed rule stated that the exclusive area agreement could cover security measures in the critical security area or restricted operations area. The final rule clarifies that these measures include §§ 107.201, 107.203, and 107.205, and would include other sections cited in those, such as § 107.207. Other responsibilities held by the airport operator cannot be assumed by the aircraft operator. An example is the provision of law enforcement support (*see* § 107.215), which can only fall to the airport operator.

In response to the question as to whether a leasehold agreement could substitute for an exclusive area agreement, the FAA believes that it is permissible if the leasehold agreement meets the criteria established in § 107.111. Such an agreement, in appropriate part, could be approved by the FAA as a part of the approved security program. Often, however, a leasehold agreement includes material not relevant to the security program, such as financial arrangements. Such information likely would have to be removed.

Comments on § 107.111(a): The RAA stated that they were very concerned about the provision that responsibility for the security of an exclusive area cannot be shared. The nature of regional airline operations often mandates that they share facilities with their major airline partners, some of which have exclusive area agreements with airports.

Atlanta Hartsfield International Airport asks if this provision will allow the assignment of access points, leading from the public area to the sterile or critical security areas, to the air carriers. They would like to have the flexibility to assign doors and portals leading to baggage make-up areas, directly to the affected air carrier.

FAA response: Like the proposal, this new section assembles all of the provisions relating to exclusive area agreements that previously appeared in §§ 107.3(b)(3), (b)(5) and 107.13. Section 107.111(a) expands the existing exclusive area responsibilities for air carriers and foreign aircraft operators to include individual access points (e.g., doors and gates). The security responsibilities for these points may be assumed by a part 108 aircraft operator, or part 129 foreign air carriers, based on a local agreement with the airport operator when approved by the FAA as a part of the airport security program.

Comments on § 107.111(b): A commenter states that nothing in this section specifically notes that the aircraft operator is directly accountable to the FAA as a regulated party for any responsibilities assumed in the agreement. This should be stated in the rule and the ACSSP.

Two airports suggest changing the word ''dimensions'' to ''general description.''

Port Authority of NY and NJ would like the flexibility to assign doors and portals leading from the baggage make-up areas directly to the affected aircraft operator.

FAA response: Complementary language in the newly rewritten part 108 (*see* § 108.227) provides that the aircraft operator is required to comply with the responsibilities in the exclusive area agreement. A failure to comply could result in enforcement action against the aircraft operator.

Section 107.111(a) exclusive area agreements, states that in an approved amended security program, an aircraft operator or foreign air carriers (one that has a security program under parts 108 or 129) would be permitted to assume responsibility for specified security measures for all or portions of the secured area, AOA or SIDA. This may include doors between baggage make-up areas and secured areas.

With regard to comments about the term ''dimensions'' in paragraph (b)(1), the agency's position remains as previously stated. In performing its

regulatory responsibility, the airport operator, aircraft operator, foreign air carriers, and the FAA must be able to distinguish clearly the boundaries of the exclusive area. This distinction is necessary in determining what security measures must be applied, and by whom.

The FAA removed proposed paragraphs (b)(4) and (5) from the final rule language of § 107.111. These sections had required that the airport operators monitor and audit the carrier with whom it had an exclusive area agreement.

Furthermore, in response to the Port Authority of NY and NJ, the language of the proposed regulation clearly allows for the airport operator as well as the aircraft operator to be responsible for doors and portals leading from the baggage make-up areas (*see* § 107.111(b)(1)).

New § 107.111(c) provides a compliance date one year after the effective date of the rule for existing exclusive area agreements to meet new § 107.111. This will give aircraft operators and airport operators time to change existing agreements to conform to the new rules. Any new agreements, however, will have to meet the new rules.

Section 107.113 Airport Tenant Security Programs

As noted in the NPRM, this new section was proposed to permit the use of airport tenant security programs. These programs allow airport tenants, other than aircraft operators regulated under part 108, or foreign air carriers regulated under part 129, to assume some of an airport operator's security responsibilities, as specified in 49 U.S.C. § 44903(c)(2). That statute also clarifies that when an airport operator chooses to implement this program, it accepts the responsibility to inspect the tenant for compliance with the tenant security program, and to take enforcement action as appropriate.

Comments: Detroit Metropolitan Airport disagrees with the notion that tenants would be responsible to the airport operator and not the FAA on security matters.

Ft. Wayne Airport states that this section should include a blanket exemption for any and all military and other Federal facilities co-located on the airport property. If they are not exempted, then close coordination between the FAA and the Department of Defense must occur prior to initiation of the new part 107 regulation.

The LSG/Sky Chefs and Lincoln Airport Authority urge the FAA to either mandate the tenant security program everywhere or eliminate this option altogether. The FAA should provide clear guidance as to what a tenant program consists of, instead of addressing the issues for the first time by each airport during the development of the program or through enforcement actions.

The ACI–NA and AAAE state that nothing in proposed § 107.113 specifically identifies tenants as the regulated party with direct accountability to the FAA for security responsibilities assumed in the agreement.

The NATA strongly opposes any attempt to regulate directly airport tenants and believes that this Congressionally-approved approach of airport tenant security programs will address the concerns of the airport operator community that were raised previously over security violations of its tenants. The penalties posed by the airport operator should not be permitted to go beyond those provided by the FAA. The tenant should not be required to enter into such an agreement with the airport, and it should be emphasized that it is voluntary in nature. There must be an allowance for the airport tenant to cancel the agreement with the airport operator.

FAA response: While Detroit Metropolitan Airport objects that tenants would be responsible to the airport operator rather than to the FAA on security matters, the statute that enacted this program provides no latitude in this regard, and was enacted largely through the efforts of an industry association.

In response to the suggestion by the Fort Wayne Airport that military and other Federal facilities at the airport be exempted, the FAA notes that Federal civilian entities are merely tenants within the context of civil aviation security. The FAA does not regulate military facilities, in that the agency's jurisdiction does not extend to military reservations. The military's cooperation in ensuring a secure airport environment is always sought. As an integral part of the host airport, the military facility, and relevant security issues, must be reflected in the airport security program.

In response to the suggestions made by LSG/Sky Chef and the Lincoln Airport Authority, there does not appear to be any reason to either require tenant security programs for all tenants or to forbid them. Each airport and tenant has different circumstances, and the use of these programs will be based on the needs and wishes of concerned parties at each airport. Within the latitude of the statute, the FAA believes such decisions are best made at the local level. However, in further response, the FAA has provided more information in the rule as to what must be in the tenant security program.

As with exclusive area agreements, airport tenant security programs would only provide for the tenant to assume responsibility for measures under § § 107.201, 107.203, and 107.205, and sections cited in those provisions. If appropriate in a given situation the airport might simply copy provisions from its own program into the tenant program. The airport operator may not transfer responsibility to provide law enforcement support. Further, the tenant may only take on employment verification responsibilities as provided in § 107.209. The tenant may not conduct the criminal history records checks, which under title 49, United States Code, section 44936, may only be done by the airport operator or aircraft operator.

Section 44903(c)(2) provides that the tenant may assume responsibility in an area that it leases or is designated for its exclusive use. The FAA interprets this to foreclose the use of an airport tenant security program for companies that contract with the airport operator to manage a terminal building. The terminal is used by one or more aircraft operators and numerous passengers, visitors, and businesses. Further, it remains the fundamental responsibility of the airport operator to provide security under the statute and the regulations for areas that directly serve the flying public. This has been made more clear in § 107.113(a). The FAA views the airport tenant security program to permit a tenant to take on security duties for areas that are not directly handling passengers for whom part 108 measures apply. It is not a means for the airport to transfer duties that are directly dealing with passengers, which is the fundamental mission of part 107. Thus, a fixed base operator at a remote site may be an acceptable candidate for an airport tenant security program. Its duties, while important to the overall security of the airport, are not as directly involved with passengers. Security at the terminal building is directly involved with passengers and should not be transferred from the airport operator.

At some airports an aircraft operator with a part 108 security program is the major or only aircraft operator at a terminal, and may lease and manage the terminal building. The aircraft operator may assume security responsibilities for that terminal under an exclusive area agreement under § 107.111.

The final rule also has been clarified to provide that only one tenant can be responsible for each area covered by a tenant security program. This is consistent with the statutory provision that the area be leased to or used exclusively by the tenant. Further, as with aircraft operators, it is evident that when responsibility is unduly diluted, it is more difficult to promote compliance with the security requirements. It should be noted that the FAA will carefully consider whether security is served before approving an airport tenant security program. Before approving the program, the FAA must find that the tenant realistically is capable of carrying out the security measures it is assuming and is willing to do so.

In response to ACI–NA and AAAE, the FAA notes that the statute does not provide for the tenant to be directly accountable to the FAA for violations. Rather, the airport operator is responsible for taking action against the tenant if it fails to comply with its security program. The term ''regulated party'' is a vague one. The tenant is regulated in that it becomes responsible for carrying out its FAA-approved security program, with consequences from the airport operator if it fails to do so.

In response to the NATA comment, the statute on which airport tenant security programs are based states that the tenant will be required to pay financial penalties to the airport operator in the event that the tenant fails to carry out any such security requirement. The statute does not address the amount to be assessed by the airport operator. The FAA's interest in this process will be served when the agency is satisfied that the program includes provisions for the imposition of fines or other penalties adequate to promote or ensure compliance by the tenant participating in the agreement.

As to NATA's comment that the tenant's agreement to an airport tenant security program should be voluntary, Section 44903(c)(2) is silent as to whether airport operators can require their tenants to enter such an agreement. The FAA generally is not involved in such tenant-landlord issues unless there are violations of Federal law, regulations, or grant assurances. As to whether the tenant will be able to cancel the agreement, if the tenant is not able or willing to carry out the tenant security program the FAA will amend the airport security program to remove the tenant security program and provide that the airport operator is directly responsible for the security measures. Any issues between the airport operator and tenant as to possible breach of contract generally will not be resolved by the FAA.

Comments on § 107.113(b): One airport suggests removal of the reference to ''monetary and other penalties.'' The airport operator must have the flexibility to resolve tenant security program infractions on a case-by-case basis.

Two airports comment that under proposed § 107.113(b)(4) tenants should be directly accountable to the FAA, if a ''person'' can be accountable.

FAA response: The tenant security program must outline the terms of the agreement, including monetary and other penalties. The reference to ''money penalties'' comes from the statute, Section 44903(c)(2)(A)(ii). The term ''other penalties'' allows flexibility on the part of the airport operator; however, the nature of that phrase must be outlined in the program by the airport operator. By the same token, the FAA will not approve a tenant security program for which the airport operator has not established a meaningful system of monetary penalties and other penalties applicable in cases of noncompliance. Further, the agency recognizes that token penalties may yield only token compliance or may be willingly incurred by some tenants as a cost of doing business. Such factors will be considered by the FAA in evaluating each tenant security program.

As to responsibility of the tenant under § 107.11, routine use of enforcement action by the FAA against the tenant would dilute the airport operator's responsibility under Section 444903(c) to make sure its security program is carried out. However, in appropriate cases, the FAA will consider action, particularly against individuals.

Section 107.201 Security of the Secured Area

The FAA proposed in § 107.201 to require the airport operator to establish a critical security area and implement certain security measures. The proposed critical security area essentially replaced the secured area that originated with existing § 107.14.

Proposed § 107.201(b) would require an identification system that incorporates the standards of proposed § 107.209 (now § 107.211), including implementation of a challenge program and escort procedures.

It was proposed that, under this section, individuals with unescorted access to the critical security area continue to be required to submit an employment verification as specified in proposed § 107.207 (now § 107.209.)

The FAA proposed that § 107.201(b)(6) require the airport operator to train individuals in a manner prescribed in proposed § 107.211 (now § 107.213) prior to authorizing such individuals unescorted access to the critical security area.

This section also proposed in § 107.201(b)(7) to require signs at access points to and along the perimeter of critical security areas. The NPRM's preamble discussion of the sign requirements referred readers to the FAA's AC 107–1 (May 19, 1972). This AC recommends that airport operators appropriately post signs warning of the entry restrictions to certain areas at the airport and any penalties associated with unauthorized entry. The FAA proposed that the airport operator be permitted 2 years to implement the new sign requirements.

Comments on § 107.201(a): One commenter states that § 107.201 should be deleted, as the systems called for in § 107.209 (Identification Systems) are unnecessary and systems identified by proposed § 107.205 (Access Control Systems) are sufficient.

The Airport Consultants Council (ACC) states that the FAA should not have different training and identification requirements for the critical security area and restricted operations area.

Another commenter asks if it is the intention of the FAA to have the critical security area replace the present SIDA. If so, the requirement for display of identification media should be completely spelled out.

FAA response: The secured area is discussed above under General Discussion of the Final Rule. As noted in the earlier General Discussion, the FAA has decided to retain the term ''AOA'' and ''secured area.'' Therefore, these terms will be used in place of ''critical security area'' and ''restricted operations area,'' respectively, for the remainder of this discussion.

Contrary to the views of the first commenter, the FAA does not believe that this section should be deleted. Proposed § 107.205, Access Control Systems (§ 107.207 in the final rule), specifies the requirements for the system, measures, or procedures for controlling entry into the secured area. An important element of strong security is redundancy. If an unauthorized person were to enter the secured area, the airport operator must have a means to determine that the person who is present is not authorized to be there; hence, the need for an identification system as provided for in proposed § 107.209 (new § 107.211). Section 107.201 establishes the secured area as

a place on the airport that incorporates these two critical security systems, as well as others, to protect the most critical operations of part 108 and part 129 aircraft operators.

In response to ACC, the FAA notes the different burdens of providing training in the secured area versus the more general requirement attached to the AOA, as noted by ACC. The agency believes that a strict training and ID standard should attach to unescorted access privileges to the secured area, where the most critical operations are performed. In other areas, there is not the same need at each airport for the most intense security requirements.

As to the commenter who asked if it is the FAA's intention to have the critical security area replace the current secured area, the FAA notes this was the intention in the NPRM. Again, however, the term ''critical security area'' has not been adopted, in favor of the current term ''secured area.''

In response to the commenters question regarding replacing the SIDA, the FAA notes that a secured area is a SIDA, and incorporates other security measures as well.

Comments on § 107.201(b): Federal Express, eight airports and one air carrier recommend changing the word ''prevent'' to ''deter and/or detect.'' These commenters believe that the program must be able to detect and remove unauthorized personnel from these areas.

One commenter states that this section implies that full badging may be required everywhere inside the fence at an airport. Such determinations should be made on an airport-specific basis in concert with local FAA officials. Badging should be based on need, not by definition of an area.

The ACI–NA and AAAE expressed several concerns regarding the proposed vehicle identification requirements.

The CALA and an airport state that § 107.201(b)(5) should be more clear and be expanded to exempt airports from having to review background investigations completed by airport tenants on persons requiring SIDA access, received from aircraft operators, that are directly regulated by the FAA.

Several airports state that this proposal should allow general terms on the signs and variations in interpretation depending upon how the airport is divided. Adding sign requirements for all doors would increase the cost significantly. Furthermore, posting signs meeting the additional criteria discussed in the NPRM would pose additional costs without any accompanying increase in security. One airport states that a minimum distance between the warning signs on the perimeter should be provided to ensure uniformity at airports. The ACC states that the proposal lacks reference to sign requirements relevant to the Americans with Disabilities Act.

FAA response: Several commenters questioned the use of the word ''prevent'' as it appears in §§ 107.201 and 107.205. The FAA disagrees with the arguments put forth by commenters. The word ''prevent'' in this context means to keep unauthorized persons and ground vehicles from the area, and appears in current § 107.13(a)(1). The section goes on to list the methods the airport operator must use to do so. The FAA believes that the high level of security required in the secured area is best completed by first preventing unauthorized access.

Further, the FAA agrees with the commenters, to the extent that a detection capability must also exist should a security system fail to prevent an unauthorized penetration or other potentially dangerous situation from occurring. This philosophy is consistent with the FAA's long held belief that the civil aviation security system is an integrated set of interdependent measures. Consequently, the final regulation also incorporates the requirement for ''detection'' in § 107.201(b), a carryover from existing § 107.13. As to the commenter who noted that the proposal implies that full badging may be required everywhere at an airport, the FAA notes that the proposal to require identification systems in both the critical security area and the restricted operations area has not been adopted. The final rule requires identification media only in the SIDA, of which the secured area is a part.

As to ACI-NA's and AAAE's questions about vehicle identification systems as proposed in §§ 107.201 and 107.203, for reasons discussed in response to comments in § 107.211, the FAA has decided not to adopt the proposed requirements for vehicle identification systems.

In response to the commenter who suggested that this proposal should allow for general terms on signs, the FAA notes its intent is to allow each local program the latitude to place appropriate signs in a manner that befits the local conditions. Signs remind the person working at the airport that they are entering an area where certain security measures are in place and for which they may be held individually accountable. Also, the signs warn the uninitiated person that access to the area beyond that point is restricted, and that security measures are in effect beyond that point. The FAA believes there is a value to the notification and deterrence effect of such signs. Consequently, the proposed language essentially is unchanged.

Section 107.203 Security of the AOA

The FAA proposed in this new section to require the designation of a restricted operations area and to specify security measures that must be implemented in it.

As in the critical security area, this section proposed that airport operators use a personnel and vehicle identification system to control movement that meets the standards prescribed in proposed § 107.209.

The FAA proposed to require that the airport operator implement the same escort and challenge procedures used in the proposed critical security area; however, access investigation would differ. This section proposed to require the existing 5-year employment history verification standards currently used in the AOA and as they appear in local airport security programs. This section also proposed requirements for signs similar to those of the critical security area.

Comments on § 107.203(a): One airport states that conducting background investigations, badging, training, and auditing all of these operators and individuals would be extremely costly, while adding no improvement to airfield security. This commenter recommends that the focus remain on security and protecting the SIDA or critical security area.

The ACI–NA and AAAE strongly recommend that the requirements formerly associated with the SIDA be limited in application to the critical security area and that the terminology be changed.

FAA response: The AOA is discussed above under General Discussion of the Final Rule. As previously noted, the FAA has deleted the proposed change to the use of the term ''restricted operations area,'' and has retained the term ''air operations area'' to reflect that area and its requirements under § 107.203. The term AOA will be used from this point on.

After further consideration, the FAA has determined that requiring identification in the AOA is not necessary at all airports, nor are the strict escort and challenge procedures that were proposed. The final rule reflects the emphasis placed on the secured area under § 107.201, as more latitude is permitted for the airport operator under § 107.203 than was proposed. However, while the measures

to be used in the AOA are not strictly prescribed by regulation, the airport operator continues to be responsible for the burden of preventing and detecting unauthorized entry, presence, or movement of persons and ground vehicles in the AOA. Some airports have decided it is necessary, with FAA approval, to require the display of identification throughout their AOA. Also, most airports require a 5-year employment history verification for those with unescorted access to the AOA. This provision, or another check to verify the person's identification, would continue to be part of the airports system to control the AOA.

Under the final rule, security requirements for the AOA remain similar to those in current § 107.13. They are: control of access to and movement on the AOA, the response to unauthorized penetrations, the provision of security information to persons with unescorted access to the AOA, and the posting of signs. The FAA believes this less prescriptive approach in the AOA will provide the greatest flexibility to the airport and its tenants. These measures generally are in effect today. The concerns of many commenters are, therefore, mitigated since part 107 airports currently possess FAA-approved security programs which adequately describe the AOA and no new burden is imposed.

Comments on proposed § 107.203(b): Two airports recommend deleting the requirement for access media for personnel with equipment within the AOA from § 107.203(b). The practicality is that this requirement will be very burdensome for small airport operators with little or no benefit to the critical security area as a result of the additional expense and manpower requirements.

Continental Airlines and the National Association of Police Officers (NAPO) state that § 107.203(b)(2) should be more thoroughly clarified and expanded to exempt airports from reviewing background investigations by airport tenants or persons requiring SIDA access. These background investigations are received from aircraft operators who are directly regulated by the FAA.

Three airports state that the posting of signs meeting the additional criteria appearing in the discussion of the NPRM would pose repetitive monetary expenditures without any accompanying increase in security. One commenter states that a minimum distance between the warning signs on the perimeter should be provided to ensure uniformity at airports.

FAA response: To the commenter who suggested deleting the requirement for access media for personnel with equipment within the AOA, the FAA points out that it is possible under the regulation and would be a local decision. For example, the FAA is aware that at some locations individuals working in teams (such as, construction crews) may not each possess individual access or identification media. Instead, such teams may work under escort of someone with the appropriate authority. The latitude for an airport operator to employ this practice continues to be acceptable under this final rule.

As to Continental's and NAPO's suggestion to exempt airports from reviewing background investigations for unescorted access to the AOA, the FAA points out that it has not adopted the specific 5-year employment verification requirement proposed under § 107.203(b)(2). Instead, the FAA chose to retain in that section the less prescriptive approach of current § 107.13 as regards control of the AOA. New § 107.203 fixes the airport operator's responsibility for the AOA to that of control of entry and movement, and the prevention and detection of unauthorized persons and vehicles.

The FAA expects that airport operators seeking to comply with new § 107.203 will need to verify the identification of persons granted unescorted access to the AOA. Since the 5-year employment verification process has provided for that for many years, some airports may choose to retain that approach. The FAA would also consider other methods to accomplish the same end.

As to the comments regarding fencing, the FAA disagrees that the costs do not result in additional security. Fences provide a positive, physical barrier to intrusions. They provide deterrence, as well as notice to well-intentioned persons who recognize that fencing sets an area apart for some purpose. Taken together with the requirements for the posting of signs under the rulemaking, the agency is convinced the two measures will provide a visible and effective means to provide an initial level of protection to the airport.

The FAA does not wish to specify a fixed distance between signs. Local conditions, the character of fence lines, topography, etc., should be more determining of sign placement than a distance set in regulation. At the same time, the FAA would expect signs to be constructed and placed in such a way as to be readily visible and readable from any point along the fence line, with details reflected in the airport security program.

Section 107.205 Security of the Security Identification Display Area (SIDA)

As noted under the General Discussion of the Final Rule, the term ''SIDA'' is being retained, but its definition is being revised.

It is the FAA's intent that airport operators who choose to apply the provisions of new § 107.209 to areas outside of secured areas must have clearly justifiable reasons for doing so. The use of the employment history verification and in some cases, criminal history records checks, under § 107.205, imposes a burden on individuals that only should be used when necessary. Examples of areas outside of the secured area that may be SIDA's include cargo make-up areas, fuel farms, maintenance areas, and other areas handling activities related to part 108 operations.

The following table illustrates the differences in security requirements between the secured area, SIDA, and AOA.

Requirements	Secured area	Security identification display area	Portions of air operations area that are not SIDA
Complex Access Controls	X		
Baseline Access Controls			X
Escort Procedures	X	X	
Personnel Identification System and Continuous Display of Identification	X	X	
Challenge Program	X		X
Employment History	X	X	
Verification and Criminal Records Check	X		X
Security Training	X	X	X
Security Briefing			X

Requirements	Secured area	Security identification display area	Portions of air operations area that are not SIDA
Signs	X	X	X

Section 107.207 Access Control Systems

This section was proposed as § 107.205 but was renumbered in the final rule as § 107.207.

The FAA proposed in this section to specify the requirements for access control systems that are required in proposed § 107.201 and § 107.203.

Proposed § 107.205(a) covered access systems for critical security areas that were essentially the same as in current § 107.14. As proposed, § 107.205(b) covers access requirements for the restricted operations area. The proposal was largely the same as the requirement in current § 107.13(a), except for the proposal that the system be locally controlled, and that the airport have accountability procedures. The proposed accountability procedures included regular audits of issued access media, and measures to ensure that access controls are locally controlled and could not be used to gain access to the restricted operations area of other airports.

Proposed § 107.205(c) addressed concerns raised by the ASAC on the issuance of temporary access media to individuals who are not in possession of their original access media. A typical example of this is an airport or aircraft operator employee who reports to work without her/his approved access and identification medium and cannot practicably be escorted throughout the course of her/his assigned shift.

Section 107.205(d) proposed that the airport operator establish and implement escort procedures for individuals who do not have access authority. Many airport operators already have some type of escort procedure in place based on FAA policy guidance, but such procedures are applied inconsistently and often ineffectively.

The FAA proposed § 107.205(e) to allow airport operators to address the issue of group validation access. The present performance standards under § 107.14(a) do not allow for group access, but the proposed language would have allowed the FAA to work with each airport operator to resolve the issue locally. Comments regarding the practicality of group access were requested.

The FAA proposed § 107.205(f) to address access control points that lead from non-public areas, other than critical security areas, to the sterile area.

Proposed § 107.205(g) would incorporate the current provisions of § 107.14(b) for alternative access systems.

Comments on proposed § 107.205 (new § 107.207): A commenter says this section is unclear and impossible to implement, while several commenters noted that the whole burden appears to be placed on the airport operator with none on the aircraft operator. An airport asks whether the proposal envisions access controls such as cameras and gate guards.

ATA is concerned about the proposed access controls for employees, particularly crewmembers, because existing controls are more than adequate.

FAA response: In response to the comment that this section is unclear and impossible to implement, the FAA disagrees. The agency wishes to point to the fact that most of the provisions of the proposal are successfully in daily use at hundreds of airports across the country under current §§ 107.13 and 107.14. As to the claim that the burden falls only to the airport operator and not aircraft operators, the FAA has long held that the responsibility to ensure a safe airport operating environment falls primarily to the airport. However, aircraft operators are required to control access to their aircraft under part 108 and, therefore, are jointly responsible for adequate security in portions of the secured area and the AOA. Further, under exclusive area agreements aircraft operators take complete responsibility for much of the security. Under this final rule, the FAA provides a means for greater relief to the airport operator through the broadened exclusive area provisions appearing in § 107.111 and with the new provision for tenant security agreements under § 107.113.

As to the exact measures to be used to control access under new § 107.207, the means by which the requirements are accomplished is largely a local decision for the airport operator, as detailed in the security program. The final rule does not specifically require the use of cameras and gate guards, although both are in common use throughout the industry today and can be a part of the systems that provide the appropriate level of security under this rule.

The FAA agrees with the ATA that the requirements for access controls under the current regulation are adequate when diligently and conscientiously implemented. For that reason, access control standards have not been expanded in the final rule. Rather, new §§ 107.201, 107.203, and 107.207 essentially reflect the access control requirements of current §§ 107.13 and 107.14.

To the commenter who objected to identification media that displayed a persons access authority, the FAA offers that this requirement has been in place for years at many airports and has proven effective. Each airport operator has flexibility to design a system that works for its airport.

Comments on proposed § 107.205(a) (new § 107.207(a)): Tucson Airport Authority states that the FAA should also address the regulatory requirement of § 107.205(a)(2) in part 108 and part 129.

ACI–NA, AAAE and two airport commenters state that § 107.205(a)(3) should be deleted, while several other airports and a local aviation department state that under § 107.205(a)(3) it would be too complex and difficult for airport employees to challenge access to different critical security areas.

One commenter questions the reasoning to allow employees to have access to only a portion of the critical security area.

Several airports reject the proposed requirement in § 107.205(a)(4) to control an individual's access to critical security area by time and date. Industry does not have the personnel required to modify access by time and date. An airport and a local aviation department state that a universal access system (UAS) for flight crews would make compliance with proposed § 107.205(a)(4) impossible. An airline states that during contingency plan operations, the issuance of special identification media limiting access by time and date could be controlled in accordance with § 107.205(g).

FAA response: As background information, the FAA notes that proposed § 107.205(a) reflects the requirements in current § 107.14(a), and represents no new requirements. The FAA agrees with the Tucson Airport

Authority that aircraft operators and foreign air carriers must notify airport operators in a timely manner of individuals whose access authority has changed. This is an element of carrying out their duties to protect their aircraft from access by unauthorized persons.

In response to the ACI–NA, AAAE, and others' comments opposing proposed § 107.205(a)(3), the requirement that the access system differentiates between individuals authorized to have access to an entire secured area or to portions of a secured area is in current § 107.14(a). The rule does not require airport operators to restrict individuals' access to specific portions of the secured areas. The rule provides that if the airport does in fact restrict access, the access control system must be capable of recognizing these restrictions. The airport is given latitude to design a system that works for its particular circumstances.

The current § 107.14(a) requires that a system be capable of limiting an individual's access by time and date has existed in the regulation since it was adopted in 1989. The proposal contained this requirement in § 107.205(a)(4). The intent was to ensure that the airport operators had a capability to limit the number of persons accessing the secured area while under a heightened or specific threat. Despite many such threats since that time, to include several during the Gulf War of 1990, the FAA has never felt the need to direct the implementation of that capability. However, it is conceivable that a threat situation may develop which could be so specific that only through implementation of this capability would the airport be permitted to remain operational. The agency notes, however, that in such a situation, the emergency authority available to the Administrator under new §§ 107.105 and 107.305 would permit the FAA to impose such requirements as necessary to respond to the emergency, as is true under current § 107.11. Hence, the retention of the disputed language is unnecessary. Its retention may impose more of a continuous burden on the industry than the worth of the measure might justify. The deletion would relieve the airports with existing systems from having to exercise, maintain, and upgrade this capability. Further, if new systems are installed, they will not have to meet this criterion.

Comments on proposed § 107.205(b) (new § 107.207(c)): ACI–NA, AAAE and several airports state that the language in the proposed rule seems to suggest that § 107.14 type controls would be required at all access points to the restricted operations area. This would be an expansion of the existing automated access control systems. These commenters do not believe that this is the FAA's intent, and request clarification of this issue.

One commenter states that if the FAA insists on the issuance of some type of airport operator access media for the AOA (proposed restricted operations areas), then a detailed justification for this identification media should be established. One airport suggests that the FAA delete the requirement under § 107.205(b)(2) and replace this with language that requires the airport operator to prevent inadvertent entry into the AOA.

UPS requests specific definition under § 107.205(b)(3) of ''be locally controlled.'' UPS requests that the system be located off property for centralization of control and reporting capability.

FAA response: In response to ACI–NA, AAAE, and others who understood the proposal to place the same level of access controls on the AOA as on the secured area, the agency notes that this is a misapprehension. Rather, the proposed rule (and the final rule, § 107.207(c)) reflect largely the same requirements on access points to the AOA as those in current § 107.13. In new § 107.207(a) of the final rule, the FAA only is to a large extent continuing the current requirements to control access to the AOA. The main addition is that the system must have an accountability system to maintain the integrity of the system. Such a system, would for instance, maintain program accountability for keys that are issued, including retrieval of the keys and re-keying the locks when necessary.

The FAA has chosen not to adopt the commenter's suggestion to delete the requirement under § 107.205(b)(2) and replace it with language which requires the airport operator to ''prevent inadvertent entry'' into the AOA. Part 107 deals directly with intentional, potentially criminal acts against civil aviation. Part 139 deals with concerns regarding inadvertent entry into or onto the AOA.

UPS asked for clarification of the term ''local control'' in proposed § 107.205(b)(3). The original concept of ''local control,'' was that a system be totally contained by the local airport or the air carrier on a local basis. When the proposed rule was written, the FAA's intent was to preclude system-wide manual access control media such as lock and key systems, in which the same access medium could be used at many airports. The danger the FAA saw, for example, was that a lost or stolen key could compromise security at all the airports where that key could operate the access control system. This has been a practice by certain air carriers in the past. The concern was a situation could arise requiring an immediate change of locks at all affected locations systemwide. This would be logistically difficult and extremely costly to achieve.

Upon review, the FAA agrees the proposal that access systems be locally controlled overstated the intent. Locks with keys that can be used throughout an aircraft operator's system may be acceptable. However, the FAA continues to object to the use of such systems that could not be altered immediately at the local level to prevent compromise of the system. Therefore, such system-wide access controls would not be approved in either airport or aircraft operator security programs unless there was sufficient local ability to alter the system as needed.

Comments on proposed § 107.205(c) (new § 107.207(d)): One commenter states that ''secondary'' access media should be renamed ''temporary'' access media, to more accurately convey the intent of this section.

UPS, Federal Express, and an airport recommend that this section be clarified to state that secondary access media can be issued when an individual unintentionally/inadvertently forgets his/her access media.

FAA response: In response to the commenter who recommends the name change, the FAA term ''secondary'' access media was chosen since it was believed to more accurately represent the fact that this privilege could be granted by the airport operator only to those persons who already have an access medium and who have already fulfilled requirements for this privilege. The use of the term ''temporary'' access media was considered but was dismissed because the FAA believes ''temporary'' implies granting of a privilege that did not previously exist and that would have a finite life. Therefore, the FAA has maintained the term ''secondary'' access media, while using ''temporary'' elsewhere in the rule (see § 107.211).

In considering the comments of UPS, Federal Express, and others, the FAA's intent in the proposed language of § 107.205(c) was to extend to the airport operator the latitude to issue ''secondary'' media. It was not the FAA's intent to require the airport operator to use secondary access media, but rather to provide the option should the airport operator choose.

Comments on proposed § 107.205(d) (new § 107.211(e)): ACI–NA, AAAE, and

several airports state that § 107.205(d)(2) should read ''* * * individuals are continuously accompanied, supervised or monitored * * *''

One airport states that escorting procedures that include group validation are flawed in that there is no means of determining who is responsible or if the group remains together.

FAA response: In the final rule, the requirements for escort appear in § 107.211.

In considering the escort function and its importance to providing for a flexible civil aviation security system, the FAA adopts the suggestion by ACI–NA and others to include the word ''monitored.'' The FAA believes the escort function can be consistently and effectively applied under this latitude at some locations. The key is whether the person monitoring the subject can immediately assess the actions of the subject and take action if the subject engages in unauthorized activity. The exact procedures may be developed at each airport and placed in the airport security program.

To the airport concerned about fixing responsibility for group escort, the FAA notes that the local escort procedures should be designed and implemented in such a way as to make clear where that responsibility lies. Further, the local escort procedures should be clear as to the actions a person providing escort should take should a person or group under escort fail to comply with the conditions of the escort.

The final rule refers to escort within the secured area or SIDA. There are some areas of AOA's, however, where escort and challenge are part of the system for controlling the presence and movement of individuals. For instance, a fixed base operator (FBO) in the AOA may monitor the activities of GA pilots and others, and challenge them if they go beyond the FBO area.

Comments on proposed § 107.205(e): Several commenters asked questions about group validation.

FAA response: Current § 107.14(a) precludes group access. The performance standards requires that each person using a § 107.14(a) access point must be tested to ensure that their authority is appropriate to the access point. At the time the changes to part 107 were proposed the operational difficulties associated with § 107.14(a) access points caused the FAA to consider permitting group access at § 107.14(a) points.

The FAA conducted tests at several locations to determine if group access through § 107.14(a) points was a viable option in light of the inherent criticality of secured areas. The results convinced the FAA that in most cases, the operational benefits offered through group access at such points could not be justified when weighed against the threat to the secured areas. Consequently, the FAA has determined that the proposed language permitting group access in § 107.205(e) is not adopted. The effect in the final rule is that only single person access will be permitted through access points that must meet the requirements of new § 107.207(a), that is, access to the secured area.

Comments on proposed § 107.205(f) (new § 107.211(e)(5)): ATA and FedEx request clarification of the areas/points included within the scope of § 107.205(f). The terms ''all points'' and ''nonpublic'' need to be defined.

ACI–NA, AAAE and an airport state that when someone accompanies a person with authorized access at that airport, the requirements of this section should not be necessary.

FAA response: The FAA has reevaluated proposed § 107.205(f). In the many cases where access points described in the proposal are indirectly controlled in accordance with current § 107.14(a) or (b), the proposed new language would require those access points to be directly controlled. Hence, a potentially burdensome requirement would have been imposed unnecessarily. The agency believes the current language is adequate for its purposes, therefore, the agency has decided not to adopt the requirement proposed in § 107.205(f).

However, as the preamble noted, there is a concern regarding a person bypassing the screening checkpoint by being escorted from the critical security area (now secured area) into the sterile area. New § 107.211(e)(5) addresses this by requiring that persons escorted into the sterile area must be screened or be escorted out of the sterile area.

Comments on the UAS: A number of comments were received on the UAS, which would allow a single access medium to be used at many airports, yet the proposed provision seems to rule out that possibility.

FAA response: The discussion in the NPRM regarding UAS was for information only. UAS has been implemented at some airports and is an on-going program.

Section 107.209 Employment History, Verification, and Criminal History Records Checks (Proposed § 107.207)

The NPRM did not contain the text of this section because it was being revised in a separate rulemaking. On September 24, 1998, the FAA issued a final rule (63 FR 51204). That rulemaking amended § 107.31, Employment history, verification, and criminal history records checks. Under the current final rule, § 107.31 has been renumbered as § 107.209 and appears under Subpart C, Operations.

Comments: Two airports state that the complexity of employment history verification requires that language should have been included in the NPRM (Notice No. 97–13) to fully assess its provisions against the other proposed changes to part 107.

Another commenter requests that the FAA continue to aggressively pursue access to the DOJ/FBI Integrated Automated Fingerprint Identification System—for security investigation—by the law enforcement entities supporting United States airports. The current program remains less than practical and largely unworkable.

FAA response: An NPRM (62 FR 13262; March 19, 1997) and a final rule (63 FR 51204; September 24, 1998) have already been issued with respect to Employment history, verification, and criminal history records check. Therefore, there was no need to republish changes associated with that rulemaking along with the NPRM for this rulemaking.

In this final rule, § 107.209 has been modified to correct an oversight that appeared in the final rule for old § 107.31. The new rule adds § 107.209(b)(3), which states that when an individual has admitted to a conviction of a disqualifying crime the investigative process ends and the individual is denied unescorted access privileges. Although this was the obvious implication of the section and the preamble, it was not clearly stated in the rule.

As to the comments submitted by two airports that sought consideration of the requirements of 107.209 within the context of the NPRM, the FAA wishes to ensure those commenters that this was done, and that the final rule reflects that process.

To the commenter that addressed the FAA's pursuit of the Integrated Automated Fingerprint Identification System, the FAA notes that it has in fact done so and tests are ongoing at this time.

The FAA receives numerous calls requesting clarification on the use of automated telephone systems that provide employment information. The FAA has contacted several of these companies and found that the information being provided comes directly from the past employer.

These telephone services provide employment information that may be

used to partially satisfy current §§ 107.31 and 108.33 regarding the employment history of those individuals seeking certain positions at an airport. The automated services provide the employment dates and does so only if the person calling has the past employer's company identification number and the specifically assigned identification number of the individual whose employment information is sought.

The use of the specifically assigned numbers reflects a level of security is being provided to the information contained within the system. The security is viewed as a means to protect the information from unauthorized changes. Since this method of providing past employment information is the ''current state of business'' the FAA will accept this method as an adequate means to verify past employment dates when the telephone services have security measures in place.

Therefore, the FAA interpretation of current §§ 108.33(c)(4) and 107.31(c)(4) and new §§ 107.209(c)(4) and 108.2(c)(4) includes the use of these automated telephone services that require the use of special information to access an individual's employment history. No language change is deemed necessary for this final rule.

Section 107.211 Identification Systems (Proposed § 107.209)

The FAA proposed that under this new section, an identification system would be required for both the critical security area and the restricted operations area. The FAA added this section to regulate standards governing the issuance, display, and accountability of identification systems to promote their effectiveness.

In addition, the FAA proposed that the standards become effective 2 years after a final rule is adopted, providing airport operators with time to make necessary changes so that their systems meet regulatory requirements. The ASAC requested that airport operators be afforded 5 years to phase in any identification changes required by the revised rule, however, the committee did not provide any financial or operational data to support this position.

In proposed § 107.209(a), standards were proposed for personnel identification media. Under this proposal, the media must convey accurate information about the individual, bear an expiration date, be readily identifiable for challenge purposes, and indicate the individual's authorization for access and movement. The FAA also proposed procedures to ensure the airport's accountability for the effectiveness of the system. It is anticipated that initial accountability criteria and percentages will have to be tested over an extended period of time and amended as appropriate.

In proposed § 107.209(b), standards were proposed for a vehicle identification system, including identification media requirements and procedures to ensure accountability of the system. At ASAC's suggestion, the FAA also proposed in § 107.209(c) to permit the use of the identification program for vehicles used under part 139, if that system also meets the requirements of this proposed section.

Under § 107.209(d) the FAA proposed that airport operators may issue temporary identification media to persons whose duties are expected to be temporary, such as contractors. To minimize the number of accountable and valid identification media, the FAA proposed that such individuals should have their identification media valid only for the time needed to perform their temporary duties.

The FAA proposed in § 107.209(e) to allow an airport operator to approve the identification media of other entities, which meet the standards of this regulation. Inclusion of this practice would codify an acceptable practice used by many airports.

Under § 107.209(f) the FAA proposed to require an airport operator to develop a challenge program. Airport operators currently establish their own challenge procedures to meet the requirements of existing § 107.25(e)(2), but in this paragraph the FAA proposed to expand these requirements in order to ensure more standardized challenge procedures between airports, and within the critical security areas and restricted operations areas.

General comments on proposed § 107.209 (new § 107.211): ACI–NA, AAAE, ALPA, UPS, ATA, NATA, FedEx, TWAA, RAA, several airports, and others provided comments concerning the identification systems. In general these commenters request greater clarification and detail in what the rule requires. ALPA recommends that an identification system cannot ''control the presence'' or ''movement'' of people or vehicles. It can only ''identify'' or ''validate'' the authority of the person or vehicle to be in the critical security area, or it can be used to ''control access.''

FAA response: The agency believes the responses to comments on specific paragraphs of § 107.209, below, provide the clarification and detail that the commenters request.

The FAA agrees with ALPA who noted that identification systems alone cannot control the presence or movement of people or vehicles. The FAA recognizes that an identification system is one of the many components of the security system. The identification media worn by persons indicate the authority of those persons to be present at given locations, and permit challenge of those without the appropriate identification. This fact, in the FAA's view, provides a means to control ''movement'' and ''presence.'' The FAA also recognizes that an identification system that relies upon display, challenge, and escort can only be as good as its users are vigilant and responsible.

Comments on proposed § 107.209(a) (new § 107.211(a)): UPS and ATA oppose application of identification requirements to flight and cabin crewmembers. They also oppose mandatory inclusion of expiration dates on media for current employees of aircraft operators. ATA states that an exemption should be allowed for flight and cabin crewmembers while they are in areas governed by exclusive area agreements. FedEx suggests that this section would place a tremendous administrative and logistical burden on the aircraft operator and crewmembers. One commenter urges the FAA to consider developing a photo identification for FAA pilot certificates in lieu of the existing non-photo based pilot certificate currently in use.

Several airports and two local aviation departments questioned the feasibility of having ''scope of access'' information on the face of the badge, particularly if there are numerous areas. To assist operators these commenters request that the FAA define ''accurate identification.'' ALPA raised the same concern and recommends that an AC be developed, or the current one amended, prescribing guidance for airport operators on the development of identification media. The AC should outline standard characteristics for all cards to make challenge easier while allowing latitude in other areas to accommodate individual airport needs. Furthermore, ALPA recommends that airport identification media be in full compliance with UAS standards, recently adopted by the FAA-chaired UAS Working Group.

ACI–NA, AAAE, and an airport agree with ASAC's recommendations that a 5-year expiration date for identification media is appropriate, particularly if the date is carried within the media itself. RAA does not support the requirement for an expiration date on personnel

identification media and requests that the FAA delete this provision.

ACI–NA and AAAE state that if audits are necessary, the FAA should consult with the industry to develop specific audit criteria and guidance documents. One commenter states that the FAA should define audit criteria, since airports need this definition to develop a system of record keeping to simplify the audit process. One airport agrees with ASAC's recommendation that 2-year audits are sufficient.

Two airports state that unaccountable badge percentages should be defined system-wide as the ''total unaccountable badges which include those lost, stolen, or not retrieved, divided by total unexpired badges issued.'' One commenter states that expired badges should not be considered as an ''unaccounted for'' badge. Another commenter states that factoring in badges with an expiration date in the unaccounted for percentage is not representative of any particular logic and requests the FAA to expand their discussion in terms of why an expiration date is necessary on a badge since airport operators are required to replace badges after a certain number of badges are not accounted for. This consideration should be a component in a cost analysis comparison for airports to upgrade their old § 107.14 systems to accommodate an expiration date on security badges.

Several airports agree with the ASAC's recommendations that the unaccountable percentages of identification badges should be raised from 5 to 10 percent. This is a more logical and rational benchmark to replace an access media badging system.

An airport states that personnel who work for more than one company that requires access to the restricted operations area should be allowed to obtain an identification card for each company. One commenter states that this gives the companies more control.

FAA response: A fundamental concept of industrial security, to include that form practiced at the nation's airports, is to establish a credible and well controlled identification system. Without such a system, there can be no surety that the persons present at or having access to a protected asset are so authorized. As discussed earlier, identification systems are useful only if unbadged persons are challenged in a timely manner. It is important to limit the number of different identification media that can be used in an area. Too many different authorized ID's, or ID's that are difficult to read, make it too hard for authorized persons to determine who is not displaying a proper ID. Expiration dates, clearly visible at a reasonable distance, contribute to a system's usefulness. With this in mind, and in specific response to ATA, the FAA will not exempt or exclude any category of person or occupation from the requirement to properly display appropriate identification in such areas as the regulation or security program mandates with exceptions noted in new § § 107.7 and 107.11. Further, a person's failure to display proper identification in accordance with an approved security program, may result in an individual becoming the subject of an FAA enforcement action under new § 107.11. This situation would not preclude other actions being taken by local authorities against the individual. Conceivably, additional culpability may attach to the regulated party responsible for control of the area in which the violation occurred.

At the same time, it must be noted that new part 108 provides a means for aircraft operators to develop identification systems that meet these standards that can be accepted by the airport operator. In this way, cabin and flight crew would not need to have a different ID for each airport, but could use their aircraft operator ID.

The FAA is not adopting the suggestion to add a photograph to the airman certificate to use it as a security tool. At best, the airman certificate would show that the person is a qualified pilot. It would not show that person's authority to be in any particular area of any particular airport.

In response to the several commenters who requested that the FAA further define ''accurate identification,'' the FAA has clarified the final rule. This information includes full name, full-face image, and identification number. The airport operator may include additional details or information at its option. Scope of access information can be displayed by using color-coded badges—a method in common use today.

In response to the commenters who addressed the issue of expiration dates, the FAA believes that clearly displayed expiration dates are an important aspect of identification media and challenge procedures. The recurring need to replace media that have reached an expiration date will afford the issuing authority the opportunity to review the holders' continued need for the media. Additionally, most identification systems will suffer some degree of unaccountability soon after implementation—identification can be lost, stolen, or otherwise become unaccounted. The unaccountable percentage generally grows over time. If expiration dates are clearly displayed, unaccountable identification media will become useless upon reaching their expiration date. Wearing an expired medium would single out the wearer as someone whose authority to be present must be challenged. The specific criteria for establishing expiration dates can be developed locally and in consideration of conditions unique to that location.

Additionally, the inclusion of an expiration date provides a benefit from a logistics standpoint. Media that have reached their expiration can be dropped from the population upon which the unaccountable percentage is based. Section 107.209(a)(3)(v) is changed in the final rule to make it clear that only media that are unexpired need to be counted for revalidation purposes.

Given the criticality of tightly controlled identification systems, the FAA cannot adopt the ASAC's suggestion that audits be performed only once every 2 years. It is not unreasonable to expect the various regulated parties to conduct comprehensive audits a minimum of once per year. In fact, such a practice is common at many airports today, while automation permits many airports to conduct audits even more frequently.

The FAA agrees with ACI–NA and AAAE that the FAA should consult with the industry to develop specific audit criteria. This will be accomplished following this rulemaking. The criteria will be incorporated into FAA-approved security programs.

The validity of an identification system is based, in part, on the idea that the media in circulation are controlled, and that only those persons who have a legitimate need for such media possess them. The validity of most identification systems can be expected to erode as media are lost, stolen, or otherwise unaccounted for over time. So, when a particular percentage of media become unaccounted for, this would represent a critical point marked as a percentage of the total population of the media. At some point, that percentage represents an unacceptably high risk to the assets the system seeks to protect. Therefore, the FAA supports the concept that the percentage figure of unaccounted identification must be based upon a common and valid formulation.

Along those lines, the FAA called for comments on what criteria should be the basis for accountability percentages. As noted in the NPRM, a range of 2 to 10 percent seems common, depending upon the nature of the venue. The FAA acknowledges the ASAC's recommendation that the traditional 5 percent maximum figure should be

increased to 10 percent, thereby allowing for a greater number of identification media to be unaccounted for before a system would need revalidation or replacement. However, the FAA believes 10 percent to be unacceptably high. Further, with technological advances, and the fact that the 5 percent figure has been in wide use for many years within the civil aviation system, the FAA sees no reason to alter that number as a maximum point at this time. However, as technologies change, and as systems are redesigned, a formula fixed in regulation may prove unwieldy. Hence, the FAA is not imposing a fixed system-wide percentage in the regulation. Since changing technologies and events may alter policy regarding the percentage, language fixing a percentage in regulation would be difficult to change in a timely fashion. Rather, the percentage will appear in the FAA-approved security programs, in accordance with FAA policy. Such programs can be modified in accordance with § 107.105. Again, at present, the FAA policy provides for a maximum allowable unaccounted percentage of 5 percent. The economic analysis for this rule has been based upon that figure.

In response to the comments on personnel who work for more than one company, the FAA has revised the language in the final rule. The revision permits the airport operator to issue to the individual such identification media as are necessary to carry out the duties of any employment the individual may hold at the airport. But, the airport operator, if it chooses to exercise that option, must ensure that its records reflect all other media issued to that individual. The FAA's intent is that any situation that would cause the airport operator to modify, suspend, or revoke any of the privileges associated with any of the individual's identification media, would also cause the airport operator to review the privileges for all other identification media issued to that individual. The airport operator would then be expected to make a finding as to whether the circumstances giving rise to the change would warrant additional modifications to other privileges held by the individual.

As to the need for retrieval of media that bears an expiration date, the FAA notes that it is not uncommon in the press of business at an airport for expiration dates to go unobserved. In order to limit the exposure to the system posed by numerous expired identification media that may otherwise appear valid, the FAA believes retrieval of expired or unnecessary media to be a prudent measure and a reasonable expectation. Where retrieval is not possible, a readily observable expiration date may provide the airport operator an added dimension of security.

Comments on proposed § 107.209(b) and (c): Several airports are concerned about the complex and exhaustive efforts that would be required of airport operators to license, catalogue and audit vehicles used in the critical security area and restricted operations area. An airport says that the cost to build and maintain a vehicle identification database and development of vehicle identification media would be significant. Federal Express, TWA and Alaska Airlines suggest that there is no case to support the inclusion of all airport vehicles in this system and that this requirement should only apply to vehicles which access the AOA from public roadways. ACI–NA, AAAE, UPS, and Federal Express state that this section and similar references to a new vehicle identification system should be deleted as they address no known security concern. Many other comments point out significant logistical and administrative difficulties with adopting a vehicle ID system.

ACC suggests the deletion of the requirement for vehicle identification altogether.

FAA response: The agency has reviewed the comments received on the proposed requirements for vehicle identification. It has come to agree with the commenters that a significant enhancement of security using this procedure at this time would not be realized. The agency believes, however, that it remains the responsibility of the regulated parties as well as individuals, all of who are now subject to new § 107.11, to assure that existing systems and procedures are applied as intended.

In light of existing requirements for control of ground vehicles under part 139, the requirements for access control in § 107.205(a) and the challenge program in § 107.209(f), the FAA believes that adequate measures are in place to identify unauthorized individuals and any vehicles they may be driving. These measures will only be successful if tenants and employees diligently apply the required measures so as to avoid incidents that may require more stringent standards.

The agency has removed the proposed vehicle identification requirements at this time, however, the FAA will monitor the situation and may reconsider vehicle identification in future rulemakings, should circumstances warrant.

Comments on proposed § 107.209(d) (new § 107.211(b)): There were no comments on this section.

FAA response: The FAA notes that the intended purpose of temporary identification is the same as for permanent identification, and as discussed in the response to comments on § 107.209(a). One difference is that the need is short term. The use of temporary identification media is not restricted to any particular class of person or occupation. The FAA believes such latitude is best left to the local authorities. Further, the agency wishes to make clear that the decision to use such media is left solely to the airport operator. The language of § 107.211(c) is only intended to place a consistent and reliable structure to such a program should it be employed.

Comments on proposed § 107.209(e) (new § 107.211(c)): ALPA states that ''Airport-approved identification media'' should be renamed ''Non-airport issued identification media'' for the sake of accuracy and clarity.

One commenter states the security program should indicate that use of aircraft operator identification media issued to flightcrew members of certificated aircraft operators is authorized for unescorted movement in the following portions of the AOA: (1) The immediate vicinity of the aircraft to which flightcrews are assigned, (2) flightcrews operations/flight office, or the equivalent; and (3) points in between, as defined in this security program.

One commenter opposes allowance of airport operators to approve the identification media of other entities that meet the standard of the regulation. This commenter would be willing to allow such media in exclusive area agreements where the entity responsible for that area permits that media.

FAA response: In response to ALPA's call to rename ''airport-approved identification media,'' the agency offers the following. For an identification medium to be accepted as a reliable indication of unescorted access authority in the SIDA, the media must be approved for the individual airport security program. For instance, an airport security program would not approve the use of an aircraft operator identification medium unless that aircraft operator was operating at that airport.

Of the airport-approved media, some are issued directly by the airport operator. Other media approved for use by the airport actually are issued by other entities such as the aircraft operators or the FAA. The main difference is the party of issuance. ''Airport-approved media'' is a term that encompasses all media, regardless of issuing party, since all such media are

cited as valid for use on the airport in the language of the security program. On the other hand, ''airport-issued media'' refers only to those physically issued directly by the airport operator. The agency believes the terminology to be properly descriptive, historically useful, and accurate. The proposed terminology is retained.

The suggestion to include language in the security program specifying the unescorted movement privilege that attach to flight crew identification media is fully consistent with a nationally mandated amendment to all FAA-approved security programs. The amendment became effective in 1993 and remains current. The new part 108 requires the same standards for identification media as part 107.

Additionally, contrary to the views of the last commenter, the FAA strongly believes that a great deal of discretion must fall to airport operators in exercising their judgment as to what other media, if any, meets the standards for approval and use within their airport security system. Since such a major portion of the responsibility for the security of the airport's surface falls on the airport operator, the FAA believes it reasonable to relegate most decisions in regard to the acceptability of others' identification to the airport operator.

Comments on proposed § 107.209(f) (new § 107.211(d)): One commenter states that challenge procedures should continue to be solely reflective of locally developed performance standards and the FAA should not micromanage the program further. The commenter urges serious reconsideration of this measure.

ACI–NA and AAAE recommend adding a subparagraph (4) under § 107.209(f), incorporating the details of the ''challenge program'' to be described in the security program.

One airport requests that the phrase ''law enforcement support'' be replaced with ''support.'' All challenges may not need to escalate to the LEO level.

FAA response: The agency is not dictating specific challenge procedures. Instead, it only proposed requiring that an acceptable local program be developed in compliance with the general language of new § 107.211(d).

The FAA concurs with the principle that the details of the challenge program should be developed locally and reflected in the security program, and § 107.211(d) so states.

The FAA agrees in part with the comment to replace the phrase ''law enforcement support'' with the less specific ''support.'' The language in new § 107.211(d)(3) clarifies that a response by other than law enforcement personnel may be included in the program. However, the airport operator continues to be obligated to ensure adequate armed law enforcement response in support of the program. This has been reflected in the final language.

New § 107.211 also includes requirements for escort, which is discussed above under proposed § 107.205(d).

Section 107.213 Training (Proposed § 107.211)

The FAA renumbered this section as § 107.213, it was proposed as § 107.211. In the NPRM, the FAA proposed that persons with security responsibilities and with unescorted access to the critical security area (now the secured area or a SIDA in the final rule) be trained similar to that current requirements under existing § 107.25.

All individuals who have unescorted access to, and movement privileges within, the AOA would be provided with information commensurate with their security responsibilities under this proposal.

In addition, this proposed section directed the airport operator to ensure that persons performing security functions for the airport are briefed on their responsibilities under the proposed rule, the security program, and any other pertinent security information.

This proposed section also specified requirements for maintaining documentation of training and the deadline for implementing a revised training syllabus.

Comments on proposed § 107.211(a) (new § 107.213(a)): One airport requests that the FAA delete the phrase ''Security Directives and Information Circulars'' from § 107.211(a). The airport operator cannot be responsible for retraining all employees every time new Security Directives or Information Circulars are issued.

FAA response: While the FAA understands the commenter's concerns, the proposal may not be as broad as the commenter may perceive. An airport operator is only required to train a person on a new Security Directive or Information Circular if the requirements and information in the document is applicable to the person's job and when that job is performed on behalf of the airport operator. A person without ''the need to know'' need not be briefed, and in fact, cannot be briefed under the provisions of § 107.101(c)(1).

Comments on proposed § 107.211(b) and (c) (new § 107.213(b) and (c)): Under § 107.211(b) and (c), the airport operator is required to ensure that all employees authorized access to the critical security area or the restricted operations area have training. Under proposed § 107.7, the airport is required to issue any FAA special agent an airport identification upon request. Commenters see this requirement as a double standard; they state that everyone requesting an airport badge should be required to complete local airport safety training. Miami International Airport states that a new airport employee can not obtain an identification badge without taking the SIDA class.

Commenters say that § 107.211(c) indicates that the airport operator would have to provide every individual a copy of the whole curriculum. Commenters hope that this is not the intent. ACI–NA and AAAE interpret the proposal to mean that each airport would develop its own curriculum, and suggest that national standards may not be appropriate at individual airports.

Several airports comment that a statement should be included to allow for ''grandfathering'' existing individuals authorized unescorted access privileges under the existing SIDA badge issuance under old § 107.25.

Another airport states that for secured areas, an individual must be trained but should not need to acknowledge the training in writing. For AOA's, they must receive information and acknowledge in writing. This seems to be putting more stringent requirements on AOA's than secured areas training.

A commenter states that the two-tiered training program, which provides less stringent training requirements for AOA personnel, has little utility. The commenter submits the differences between the two to be minimal and states that a more conservative higher level training standard approach does no harm.

FAA response: The FAA understands the commenters concerns regarding issuance of an airport identification upon request of any FAA special agent. As discussed more fully under § 107.7, the agency agrees that under routine circumstances, appropriate safety and security related training should be provided to FAA special agents before they exercise full access privileges to an airport. Such training can be provided at the airport which is the agent's primary duty location and can be supplemented with local training at other airports requiring such training. This approach is in common use today throughout the industry for persons requiring similar access privileges. In emergency situations, such as in responses to hijacking situations, the responding agents may not have the opportunity to

be provided the training or access media for that particular airport. The exigencies of their unique duties in such circumstances may override other considerations and the language of the final rule has been modified to permit this.

New § 107.213(c) does not require that each trainee be provided the whole curriculum. The intent is to ensure that employees have been provided all relevant information in accordance with the security program. The relevant information can be given in writing, by videotape, a personal briefing, or any other means the airport operator chooses to provide the information to the individual. The FAA agrees that each airport would develop its own curriculum.

The rule does not provide that all individuals who have already taken training under current § 107.25 may be ''grandfathered.'' Each airport will have to evaluate whether there have been changes, for example, designations of areas as AOA or secured area. If changes are made, the airport must train those individuals who need to comply with the new conditions.

In regard to the comment that the proposal on training acknowledgements seems inconsistent on its face, persons receive the more definitive training required for unescorted secured area and SIDA access in a more formal, classroom-like setting, with the ability to ask questions. The airport operator can directly observe whether the person has successfully completed that training.

Conversely, persons receiving information necessary for AOA access may do so in a less formal, more self-study process in which case an acknowledgement by the trainee would be an appropriate record. However, it is evident that training under § 107.213(c) may also be in a classroom setting. The final rule in § 107.213(d) does not require an acknowledgement by the trainee under § 107.213(c), it only requires that a record of training given to each individual be maintained.

In regard to the comment on the two levels of training, the FAA has sought to provide for an option to train those with access to the AOA only using a lower-cost method. Should an airport operator wish to exceed the minimum required training standards and require more formal training, the FAA would be supportive.

Comments on proposed § 107.211(e) (new § 107.213(f)): One airport is concerned that proposed § 107.211(e) would allow all training to be dropped for the 2-year period prior to the effective date of the rule.

FAA response: After further consideration, it appears that the only new feature in § 107.203(b) for training for persons with access to secured areas or SIDA's is training in § 107.11. Therefore, new § 107.213(e) provides that for persons who already have such access, classroom training will not be required. The airport operator need only to provide them information on § 107.11. Providing information under new § 107.213(e) is a new requirement, but is less complicated than the § 107.213(b) training. Airports will have 1 year to implement this program.

Section 107.215 Law Enforcement Support (Proposed § 107.213)

This section was renumbered in the final rule as § 107.215, it was proposed as § 107.213. In the Notice, this section specified the qualifications of law enforcement support required under proposed § 107.103, which were similar to those in current § 107.15. The most substantial change made to this proposed section was the distinction between the use of uniformed and ''plainclothes'' law enforcement personnel.

Comments: Phoenix Aviation Department, Tucson Airport, and Port Authority of NY and NJ request more flexibility for airport operators to be permitted to respond with ''plainclothes'' officers provided appropriate insignia/badge is displayed when necessary. The FAA was urged to reconsider the uniformed concept and allow plainclothes LEO response, while airports should be expected to maintain a visible uniformed presence throughout the airport environment.

ALEAN and two airports request the FAA to delete references to ''in the number and manner'' in § 107.213(a). Several airports state that the number of officers necessarily is a local decision.

Alaska Airlines recommends that the airport law enforcement and aircraft operator should establish a triage type system for LEO response. Two airports state that § 107.213(b)(1) should be clarified to state that LEO's are to be available to respond to an ''airport security related'' incident. Another airport states that § 107.213(b) is a general and non-specific section and could mean response at anytime to any location on the airport. If this section is referring to the screening checkpoint, it should state that.

ATA and RAA support the requirement that, on request of an aircraft operator or foreign air carrier, certified law enforcement personnel should respond to an incident.

FAA response: In response to the commenters who urged the FAA to reconsider its position on the use of only uniformed law enforcement personnel for the response to the screening checkpoint, the agency points out that the language of the regulation does not preclude the use of plain-clothes officers to supplement a uniformed response, or to supplement or comprise a complete response to any other situation. Regarding a response to the checkpoint, however, the value of a uniformed law enforcement presence in terms of deterrence, ease of recognition during an emergency situation, and in sustaining the confidence of the public, cannot be overstated. The FAA insists that this capability continue.

The FAA recognizes that the ''number and manner'' in which law enforcement personnel are provided is largely a local determination under new § 107.215(a)(1). The FAA looks to whether law enforcement responds to screening checkpoints, alarming doors, and other events in a timely manner, as well as providing adequate security patrols.

In response to Alaska Airlines and others, the FAA notes that proposed § 107.213(b) (new § 107.215 (b)) applies only to those airports identified in § 107.103(c). Such airports normally do not have airport law enforcement on site and only have limited passenger operations that would require screening and law enforcement support. The wording in the proposal is essentially unchanged from the current § 107.15(b) and refers to a law enforcement response for any reason in support of the civil aviation security program. The FAA sees no need to modify the language or to require a ''triage system'' as suggested.

Section 107.217 Law Enforcement Personnel (Proposed § 107.215).

In Notice 97–13, this section was proposed as § 107.215. It has been renumbered as § 107.217 in the final rule. As discussed in regards to proposed § 107.213 above, the requirement for all law enforcement personnel to be in uniform was modified. To reflect the proposed change it was proposed that § 107.215(a)(2) not include the uniform requirement as appears in current § 107.17(a)(2).

Proposed § 107.215(c) updated training requirements in current § 107.17(c) for State and local law enforcement officers to reflect the fact that all states have law enforcement training programs. This proposed paragraph also specified that private security personnel used to meet the requirements of part 107 must be trained in a manner acceptable to the

Administrator if the State and local jurisdiction does not prescribe training standards for such personnel.

Comments on proposed § 107.215(a) (new § 107.217(a)): NAPO and Monterey Peninsula Airport are concerned that there will be substantial replacements of law enforcement officers (LEO's) by less experienced and inadequately trained private security forces. NAPO states that the FAA should not generate a rule inviting substantial replacements of experienced and well-trained LEO's which will have potentially serious consequences on airport and aircraft operator security. NAPO recommends that the FAA specify areas of the airport and situations mandating the presence of LEO's and also require a minimum contingent of LEO's at each US airport. One airport suggests replacing the word ''indicia'' with ''appropriate badge or uniform of authority.''

FAA response: The FAA does not have the latitude to provide for the concerns raised by the NAPO and other commenters. The term's ''law enforcement personnel'' and ''indicia of authority,'' as reflected in proposed § 107.215 (new § 107.217), were established under Title 49, United States Code section 44903. The statute authorizes the operator to use the services of qualified State, local, and private law enforcement personnel. The regulation is revised to be consistent with the statutory language.

Comments on proposed § 107.215(b) (new § 107.217(b)): Miami International Airport, UPS, ACI–NA, AAAE, and others comment that the FAA should provide for local law enforcement officers to be ''deputized'' to enforce federal regulations. Some of the commenters' note that LEO's are more often called to respond to incidents such as interference with flight crews, where they have no authority to take action nor are they supported by the statute.

FAA response: Situations such as cited by Miami International Airport and other commenters fall outside the scope of this rulemaking. The FAA notes, however, that nothing in the final rule precludes having law enforcement personnel deputized to enforce selected Federal statutes. Further, there are some airports at which selected airport police officers have been deputized by the United States Marshal Service.

Comments on proposed § 107.215(c) (new § 107.217(c)): Two airports request a deletion of the reference to ''LEO's'' from § 107.215(c). Another commenter recommends retaining the title law enforcement ''officer'' instead of law enforcement ''personnel.'' Miami International Airport states that LEO is a recognized term within the industry. ALEAN states that the term ''private law enforcement personnel'' is confusing and problematic. The phrase should be ''private security personnel.''

Tucson Airport and Phoenix Aviation Department request clarification of what constitutes adequate training under this section. Two airports and a port authority request removal of reference to ''any other subject the Administrator determines is necessary,'' stating that this gives the FAA a blank check to do anything.

FAA response: As explained previously, the use of the terms ''law enforcement personnel'' and ''private law enforcement personnel'' are consistent with Title 49 U.S.C. § 44903. To be qualified for this task, law enforcement personnel (whether state, local, or private) must have the arrest authority, weapons authority, and training set out in this section. The term ''private security personnel'' often is used for uniformed persons who are not armed and do not have arrest powers, and is not suitable for this section. The FAA knows of at least one airport jurisdiction in which law enforcement support had been provided to the airport operator under contract by a private firm. There, privately employed individuals were granted arrest powers and in all other respects meet the requirements for law enforcement support as outlined in this statute and part 107.

In response to the Tucson Airport, the FAA notes that the language of the final rule, in effect, leaves to the local jurisdiction the determination as to what constitutes ''adequate training'' for publicly employed LEO's. In the case of private law enforcement personnel serving the law enforcement role required under this part, the Administrator must approve their training, and must, therefore, determine the adequacy of their training.

With respect to the phrase ''any other subject the Administrator determines is necessary,'' the FAA Administrator reserves the right to add to the training program. The changing nature of the civil aviation security program, and of terrorism or other criminal threats in general, may generate the necessity for additional training in the future that cannot be anticipated at this time.

Comments on proposed § 107.215(d) (new § 107.217(d)): Five airports state that the FAA should remove reference to ''principal operations office'' and add ''as detailed in the security program.'' The place of retention of training records is a matter of legal guidance and operational needs and preferences.

Another commenter states that police training records should be maintained by airport police personnel. A commenter asks who pays for maintaining the training records required by this paragraph.

The Tucson and Phoenix Airports question the means and resources of training under this section.

FAA response: The FAA concurs with the commenters' concerns regarding the location of the records. The final rule does not specify the location of the records.

The final rule does not require the airport operator to possess the actual records, it only requires that they be available for review upon request in accordance with § 107.7(a)

The rule does not specify who will absorb the costs for maintaining the training records. Likely, this will depend on what entity maintains the records.

Section 107.219 Supplementing Law Enforcement Personnel (Proposed § 107.217)

In the Notice, this section appeared as § 107.217; it has been renumbered in the final rule as § 107.219. Under the proposal, existing § 107.19 entitled ''Use of Federal law enforcement officers,'' was revised and renumbered as § 107.217, ''Supplementing law enforcement personnel.'' This revised section sets forth the same procedures for an airport operator to request Federal assistance in supplementing local law enforcement, and has incorporated statutory language that would provide for supplemental support from any personnel employed by the Federal government.

Comments: Commenters suggest that the idea of supplementing airport LEO's with Federal officers is fraught with problems including jurisdiction, legal authority, training and availability. The NAPO recommends that the FAA should reconsider its clarification of statutory authority to allow for wholesale substitution of governmental LEO's in all airport locations under most circumstances and situations. Another commenter suggests that § 107.217(b) should be removed because the statement is too broad and serves no interest.

FAA response: New § 107.219(a), which remains unchanged from the proposal, is intended to provide emergency law enforcement support to airport operators where local law enforcement is either no longer available or is not adequate to meet the requirements of an emergency situation. While this provision has existed in regulation for many years, it has not yet

been invoked. Commenters are referred to Title 49 United States Code section 44903(c).

The basic information required by § 107.219(b) is intended to help the Administrator decide whether or not to supplement local law enforcement personnel and to prioritize assignment of resources in the event multiple requests are received. The specific requirements of paragraph (b) are directly related to Title 49 United States Code section § 44903, and therefore must be retained.

Section 107.221 Records of Law Enforcement Response (Proposed § 107.219)

This section has been renumbered in the final rule as § 107.221; it was numbered as § 107.219 in the proposed rule. The FAA proposed that § 107.219 would incorporate new recordkeeping requirements found throughout the proposed rule and ensure that the FAA has access to such records.

Under proposed § 107.219(a) the FAA would have access to any record required under the proposed rule and would require the submission of records to the FAA pursuant to a schedule approved in the airport's security program.

A slight modification was proposed for records resulting from law enforcement activity. In proposed § 107.219(b)(l), the word ''action'' was changed to ''response.'' Proposed § 107.219(b)(2) extended the period of time during which records must be maintained to a more practical 180 days. It was also proposed in § 107.219(c) to require records to include more specific information about individuals who are detained or arrested. This information would aid the FAA and the FBI in the investigation of such incidents and in the analysis of data as a management tool.

The addition of proposed § 107.219(d) would require the airport operator to make and maintain for 180 days records of any corrective action taken against persons who fail to comply with falsification and security responsibilities under § § 107.9 and 107.11. A new § 107.219(e) was also proposed to require the airport operator to maintain any additional records that may be needed to support the security program, and highlight additional recordkeeping requirements found throughout the proposed rule.

Comments on proposed § 107.219(a): Three airports, a port authority and an aviation department request that the FAA replace the word ''furnished'' with ''made available.'' Another commenter states that § 107.219(a) should be deleted, and add ''Records required to be maintained should be made available to the Administrator upon request.''

One commenter states that increasing record creation/maintenance requirements for the pleasure of the FAA incorporates no increase in security posture while encroaching upon visible patrol time and availability of personnel for timely response to needs for LEO services.

FAA response: After further consideration, it is evident that new § 107.7 provides for inspection by the FAA of records used to show compliance with this part. Therefore, proposed § 107.219(a) is not needed and is not adopted.

Comments on proposed § 107.219(b) (new § 107.221(a)): The Airport Consultants Council (ACC), an airport, a port authority, and a local aviation department state that the FAA should consider more realistic record retention requirements and strongly urges the FAA to reassess the across-the-board 180-day timeframe and develop a more logical retention matrix associated with the type of information. Another commenter recommends maintaining the current 90-day requirement. A commenter states that the vast majority of the records required in this section is generated at the security checkpoint and would be best supplied and retained by the aircraft operator and their contractors. Another airport states that records for police actions should be the only requirement as there are a significant number of responses where no action is taken. Metropolitan Washington Airports Authority requests that the FAA replace the phrase ''law enforcement response'' with ''law enforcement action.''

FAA response: This paragraph is renumbered § 107.221(a) in the final rule. The FAA's 180-day timeframe is intended to ensure that the subject records are maintained during what is expected to be the maximum period between regularly scheduled FAA inspections. It is hoped that this interval will ensure that records are available when and as needed for FAA purposes.

The records required by this section refer to law enforcement records. The FAA agrees with the substance of the comment that only certain actions taken in support of the security program should be provided to the FAA, while other records need only be made available upon request. Therefore, the final rule requires that records be made of law enforcement ''actions'' instead of the broader category of ''responses.'' The specific types of records that the FAA expects the airport operator to provide routinely, in accordance with the schedule included the security program, would include actions taken in support of the security program and that result in arrests, detentions, or discovery or confiscation of weapons, explosives, and incendiaries.

Comments on proposed § 107.219(c) (new § 107.221(b)): The ACC and an airport state that § 107.219(c)(4) is too broad a category. The FAA needs to assess the validity of retaining this information. One commenter suggests the FAA provide a process to gather and store relevant statistics in a timely manner.

FAA response: This paragraph is renumbered § 107.221(b) in the final rule. The FAA disagrees that the information cited under the proposed rule is broad. Rather, it believes that such information in 107.221(b)(4) is specific, and is routinely developed for each instance of detention or arrest. The agency believes this information is necessary to identify trends, and to meet reporting requirements placed upon the FAA by other entities, to include the Congress.

Comments on proposed § 107.219(d): FAA is not adopting language related to a compliance and enforcement program as proposed under § 107.103, at this time. Such issues will be dealt with in a later rulemaking action.

Comments on proposed § 107.219(e): An airport, a port authority and a local aviation department suggest that the FAA delete the phrases ''maintain any additional records'' and ''but not limited to'' in § 107.219(e). Any new requirement for maintaining records should be introduced through the rulemaking or amendment process with sufficient time to implement the recordkeeping procedures.

FAA response: The FAA agrees that any additional reporting requirements, particularly as levied by entities with authority over the FAA, such as, the Department of Transportation and the Congress, would not be so time critical that a more deliberate approach is precluded. The agency, therefore, recognizes that airports would need time to comment on and to implement any additional recordkeeping procedures beyond that already specifically required in regulations or security program language. Proposed § 107.219(e) is withdrawn.

Section 107.301 Contingency Plan

This proposed new section would require airport operators to implement FAA-issued contingency measures contained in their security programs when directed by the Administrator. It also proposed that airport operators (and aircraft operators under parallel

language of part 108) should test these contingency plans to ensure that all parties involved are aware of their responsibilities and that information contained in the plan is current.

Comments: Sacramento County Department of Airports requests clarification of the Contingency Plan and asks whether the FAA expects airports to replace the Aviation Security Contingency Plan (AVSEC).

ACC requests that the FAA update its alert levels and contingency measures.

An airport and a port authority state that the term ''exercises'' should be removed from the phrase, ''conduct reviews and exercises.'' Then the regulations would parallel to existing part 107 and part 139. Another commenter recommends an annual requirement to review and exercise the contingency plan.

Two airports state that § 107.301(b) should specify that table top exercises instead of the application of measures with real events is sufficient to meet the requirement for reviews and exercises.

One commenter states that it is the FAA's responsibility to ensure that invited parties participate in contingency plan reviews and exercises. Another commenter recommends that aircraft operator participation should be addressed in part 108.

FAA response: The current AVSEC Plan is mandated by a security program amendment. The FAA does not expect the airports to replace the AVSEC Plan based upon this rulemaking. Rather, this proposal language was intended to clearly state the regulatory foundation for the existing plan.

The FAA disagrees with the commenter who suggested removal of the requirement for airport operators to conduct ''exercises'' of their contingency plans. The FAA developed the AVSEC Plan to ensure that the FAA, airport operators, aircraft operators, and other affected parties are able to respond effectively and on short notice, to each threat to civil aviation security. A contingency plan, in order to be most effective, must be rehearsed regularly with all key participants and infrastructures involved. The FAA experience has shown this approach will help to ensure a timely response to actual threats, therefore, the requirement to perform ''exercises'' will remain. The agency expects that such exercises will be conducted in accordance with requirements established in local security programs.

The airport operator has a responsibility to ensure that all key participants, including aircraft operators, are knowledgeable about the contingency plan and participate in exercises. Consistent with this, aircraft operators have a responsibility under § 108.301 to develop and practice the contingency plan and to participate in tabletop exercises of the airport plan. The FAA views its role as ensuring that all parties to this plan maintain a state of preparedness necessary to respond to reasonably foreseeable situations. The agency believes the regulation, as modified, promotes that end.

Section 107.303 Security Directives and Information Circulars

This proposed new section would correspond to proposed § 108.305 and requires airport operators to respond to Security Directives in the same manner as aircraft operators.

The FAA has used Security Directives as a means to disseminate information to aircraft operators concerning security threats and to require appropriate measures to be implemented. The FAA uses Information Circulars for the notification of general information regarding threats to civil aviation security.

This section also proposed to permit the ASC to apply for a security clearance through the FAA in order to receive classified information related to national security.

Comments on § 107.303(a): One airport states that § § 107.303(a) and (b) are inconsistent. Paragraph (a) refers to the Assistant Administrator issuing a Security Directive and paragraph (b) refers to the Administrator issuing a Security Directive. Another commenter states that the language should be amended to account for the fact that the Administrator issues Information Circulars to convey threat information.

One commenter states that the type and quality of threat information provided to the airport operators is barely useful in security practices.

One port authority states that the FAA should specify in the language that all Security Directives will be addressed to the ASC and/or their designated alternate.

One commenter states that there should be some distinction made between airport and aircraft operator Security Directives.

FAA response: The FAA agrees that there were apparent inconsistencies in the language. The final rule has been amended to reflect that all actions are taken by the Administrator. However, under § 107.1(b) the Administrator's authority is also exercised by the Assistant Administrator for Civil Aviation Security or the Deputy Assistant Administrator for Civil Aviation Security. Section 107.1(b) also addresses further delegation of the Administrator's authority.

In response to the commenter that stated that threat information is ''barely useful,'' the FAA notes that it makes every effort to provide useful threat information to all regulated parties. However, much of the information upon which Security Directives and Information Circulars are based may have been classified by other Government agencies. Consequently such information can only be released if it has been crafted in such a way as to protect the interests of those agencies. The ability of the agency to grant a Federal security clearance to certain airport officials allows greater latitude in passing on more specific, and hopefully more useful information.

Further, often the information the government holds is very limited, and there is little more specific information to pass along. In such a case, the FAA provides what information it can to keep the airport operator as informed as possible.

The FAA agrees with the commenter that the ASC plays a crucial role in the chain of communication. The final language of the regulation reflects in § 107.5(b)(1) the ASC as the point of contact for this purpose, however, other officials at the airport may also receive information at the FAA's discretion and based upon the circumstances.

The FAA agrees with the commenter who notes that confusion could result when more than one type of regulated party receives a similarly titled document. The FAA also recognizes that the Emergency Amendment process has been used for the notification of both airports and foreign air carriers regulated under part 129. The agency notes that the language of the documents generated under this provision will clearly indicate their applicability and intent.

Comments on § 107.303(b): One airport and a local aviation department state that airports should have a minimum of 3 business days to comply with Security Directives.

FAA response: The FAA does not believe it is appropriate to provide in the regulation a minimum of 3 business days to comply with Security Directives. Security Directives usually respond to an immediate threat. Hence, the FAA will not place regulatory constraints upon its ability to be responsive in these situations. It will, however, be mindful of the difficulties in complying with contingency measures and will permit additional time for implementation where the circumstances of the situation permit.

Comments on proposed § 107.303(c): One commenter strongly opposes § 107.303(c) that presumes to regulate the airport via the Security Directive.

One airport states that a Security Directive cannot be implemented in ''24 hours.'' Another commenter suggests replacing the references to ''24 hours'' or ''72 hours'' with references to business days (such as, 1 day or 3 days). Miami International Airport suggests that ''24 hours'' and ''72 hours'' should refer to business hours. Smaller airports are not continuously staffed and may not receive a Security Directive until resuming normal workday hours. Otherwise, the FAA must be required to contact the airport to advise that a Security Directive is being transmitted.

One commenter strongly disagrees with the time requirements to comply with a Security Directive. Any significantly intrusive or expensive measure would only need to be implemented if the airport, aircraft operators and the FAA agree that the threat justifies the action.

One commenter states in regards to § 107.303(c)(3) that airports should only be responsible for advising employees directly employed by the airport with a need to know (those on the payroll).

FAA response: The Security Directive process, like the Emergency Amendment process that has been in use for years, is intended to respond to imminent threats. The FAA cannot categorically state in this rule that in each case the airport should have a specified number of hours or days to implement the measures. The FAA is aware that each case must be evaluated, and the circumstances of each airport must be considered, in determining compliance times.

The FAA disagrees with the commenter who addressed § 107.303(c)(3) in that the airport operator may be the only appropriate authority to pass on such information, especially to persons not employed directly by the airport operator or an aircraft operator. The airport operator may also be the only authority in the position to design, describe, and institute appropriate measures. Further, the airport operator has control over such critical functions as the access systems and identification systems. As such, the duty to provide such details to persons having the need to know would logically fall to the airport operator.

Comments on proposed § 107.303(d) and (e): There were no comments on these paragraphs.

Comments on proposed § 107.303(f): Another commenter strongly supports receiving classified information after the ASC has applied and received a security clearance.

FAA response: The proposed language was intended to highlight this option. However, the language has been deleted in the final rule simply because it is unnecessary. The FAA wants to make it clear that the option for the airport operator to receive classified material by an appropriate designated official still exists, and the FAA actively encourages the exercise of that privilege.

New § 107.303(e) makes clear that the airport operator may submit written comments on a Security Directive. The FAA currently receives many verbal comments on Emergency Amendments, and expects to continue to receive verbal comments on Security Directives issued to airports. This often is a quick way for industry and the FAA to exchange information on the practical impact of the Emergency Amendment or Security Directive and for the FAA to provide guidance, and make changes to the Emergency Amendment or Security Directive as needed.

Section 107.305 Public Advisories

This proposed new section was added to incorporate new statutory language and a 1986 security program amendment.

Comments: ASAC and six airports recommend that the most effective means to notify passengers of public advisories is to flag those foreign airports on airline reservations systems. The booking agent would then notify the passengers verbally that the destination airport does not meet FAA standards.

Three airports and a local aviation department recommend that the aircraft operators should be responsible for posting warnings in the ticket jacket. A part 108 requirement to advise passengers via ticket sleeve inserts would diminish airport signage costs, information overload and clutter.

One airport asks why the security program has to specify the timeframe that the public advisory shall be posted? It is meaningless to have an arbitrary time of posting in the security program. Another airport states that by the time the passengers see the sign, they have checked in and committed themselves to the trip.

FAA response: The requirement to provide public notification at US airports that a foreign airport has been determined to have failed to maintain or carryout effective security measures is found in the Title 49 U.S.C. 44907(d)(1)(ii)(A). Under this statute the notification also is published in the **Federal Register** and the news media is notified. The FAA believes that posting the identity of that airport is best accomplished by a single entity at each location. That entity is determined to be the airport operator. The law also requires aircraft operators to notify their passengers of that foreign airports' status.

As to the question regarding timeframes for postings, the rule provides that the period of time is determined by the Secretary of Transportation.

Section 107.307 Incident Management

This new section was added to require the airport operator to establish procedures to evaluate and respond to threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

Proposed § 107.307(b) would specifically provide that the evaluation of a threat would be conducted in accordance with the security program. However, any event covered by the part 139 airport emergency plan, such as an actual hijacking, would be handled as specified in the airport emergency plan.

To promote coordination between part 107 and part 139, the FAA also proposed to amend § 139.325 to ensure that emergency response procedures to hijack and sabotage incidents contained in the airport emergency plan are consistent with the approved security program. Proposed § 107.307(d) supported this coordination by requiring the airport operator to review annually threat and incident response procedures. Such a review is intended simply to ensure threat response procedures and contacts are still accurate and should not be interpreted as a requirement for a full-scale exercise.

In the event that an airport required to have a security program under part 107 is not required to have an airport emergency plan under part 139, proposed § 107.307(c) would require the airport to develop emergency response procedures in addition to threat evaluation procedures.

Comments: The Sacramento County Department of Transportation and two airports recommend deleting § 107.307. An airline suggests that § 107.307(a) could lead to disputes between the aircraft and airport operators as to who should actually evaluate bomb threats against flights and aircraft. One commenter recommends removing the phrase, ''As described in the security program'' from § 107.307(a) since it is unnecessary.

FAA response: The FAA agrees that the proposal was not clear as to the airport's role in evaluating threats made to air carriers. The final rule states that

the airport operator must evaluate or take action on only those bomb threats it receives directly, or that are referred to the operator by any other entity. For example, should an aircraft operator receive a bomb threat that it evaluates under the provisions of § 108.303 and determines that the bomb threat is neither specific nor credible, it need not refer the bomb threat to the airport operator. However, if the aircraft operator refers a threat to the airport operator or if the airport operator receives a threat directly or by other means, the airport operator is obligated to act under the provisions of § 107.307.

The FAA also agrees with the commenter's request to delete the opening phrase ''As described in the security program'' from § 107.307(a). Since the implementing details of almost all requirements appearing in part 107 are placed in the FAA-approved security program, the insertion of the subject language in § 107.307(a) is unnecessary.

Part 139—Certification and Operations: Land Airports Serving Certain Aircraft Operators

Section 139.325 Airport Emergency Plan

The FAA proposed to add a new section, § 107.307, to require the airport operator to establish procedures to evaluate and respond to threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations. Existing part 107 lacks a specific requirement for airport operators to respond to threats of such criminal activity. Instead, part 139, Certification and Operations: Land Airports Serving Certain Aircraft Operators, requires airport operators to be prepared to respond to an actual incident of sabotage, hijack, and other emergencies by developing and testing an airport emergency plan under § 139.325. These emergency procedures are sometimes incorporated in the security program verbatim, and generally speak to emergency services responses.

The FAA believes that emergency response procedures to such incidents such as bombing or hijacking, should remain in the part 139 airport emergency plan. An expedited response to emergency situations is critical, and response procedures to any emergency should be limited to one document to minimize delays and confusion.

To promote coordination of the procedures to implement the requirements of part 107 and part 139, the FAA proposed to amend § 139.325 to ensure that emergency response procedures to hijack and sabotage incidents contained in the airport emergency plan are consistent with the approved security program.

Comments: One commenter recommends removing the requirement to have the airport operator to obtain two approvals for its security program (FAA Security Division and FAA Airports Division). Another commenter recommends excluding all emergency plans dealing with security, stating that security emergency plans belong in part 107 only. Another commenter states that the consensus of the airport community is to remove any cross-reference between part 107 and 139.

One commenter states that part 139 does not have protection under the non-disclosure rules.

FAA response: Nothing in this rule requires the airport operator to obtain two approvals for its security program. The changes to § 139.325 require the airport operator to ensure consistency between the operator security program required under part 107 and its airport emergency plan under part 139. The purpose here is to prevent confusion and contradictory program language that would hamper rather than facilitate any response to an actual emergency situation at the airport.

The FAA disagrees with the recommendation to exclude all emergency plans dealing with security. The security program under part 107 is intended primarily to detail how the airport operator will prevent or respond to emergency situations. The airport emergency plan focuses on the emergency services response to a situation that has already occurred. Since the emergency plan deals primarily with emergency medical services, fire and rescue services, etc., the concerns are unique to that program and are properly included in that plan. The FAA recognizes some areas of overlap, but the programs and their purposes are distinct enough that the FAA believes they deserve their own separate document with review by the FAA specialists versed in their respective fields of expertise.

In response to the comment about protection under the non-disclosure rules, any sensitive security information as defined in part 191 that may be contained in the emergency plan must be protected in accordance with that regulation.

Summary of Economic Comments

This section will summarize the economic comments and the FAA's responses. A detailed discussion of these comments and responses is contained in the full evaluation in the docket for this proposed rule. A total of 66 commenters raised economic issues.

General comments: Two commenters believed that the numbering and ordering of several sections changed since the analysis was originally done.

One commenter could not understand why the FAA avoided any cost estimation for the effects of §§ 107.31 and 108.33.

One commenter notes that the NPRM's economic summary states that the proposed rule ''is not a significant rulemaking action,'' and so asks, then why are we doing it?

One commenter objected to the FAA using 1994 FAA forecasts for a document that was not published until 1998.

One commenter believes that the proposed regulations would have an impact on international trade.

Two commenters believe that the costs of these regulations will result in yet another unfunded mandate.

FAA response: No specific examples were given of how the scope had changed. One commenter did submit a chart, which purported to show these differences. In this chart, most of the differences were explained in terms such as ''not the same,'' ''increased scope,'' or ''potential reduced flexibility''. Without specific examples, the FAA cannot respond to this commenter's concerns.

The FAA has provided cost estimates for §§ 107.31 and 108.33 in the analysis for the ''Unescorted Access'' final rule.

The Office of Management and Budget (OMB) and the Department of Transportation (DOT) have specific definitions for ''significant'' rulemaking actions that include certain cost and/or policy criteria. The fact that this rulemaking does not meet these criteria does not mean that this rulemaking action is irrelevant.

Even in the best of times, given the limited resources within the FAA and DOT, it is often normal for there to be a delay between the time that the analysis is done and published.

Unlike air carriers, airports are not in competition with their foreign counterparts.

As required by Congress, the FAA has examined these regulations in light of the Unfunded Mandates Reform Act of 1995 and found that this Act does not apply.

Comments on the assumptions used in the analysis: Two commenters questioned the assumption that the number of airports and their distribution into airport types would not change for the 10 year span of the analysis.

Four commenters believe that using data from many different years, such as 1989, 1991, 1992, and 1994 is inappropriate for a 10-year projection to 2009.

Two commenters were uncomfortable that data was used from an analysis dealing with testing for alcohol usage.

Two commenters believe that the number of badged staff used in the NPRM analysis were incorrect.

One commenter stated that the assumption that all identification media will be magnetic stripe is unrealistic.

One commenter believed that the FAA's assumption that it would take 1 hour to reissue a card assumed no queuing and thus was too low.

One commenter claimed that the discount and price deflator numbers needed clarification and standardization.

One commenter objects to the FAA grouping airports into Types A, B, and C airports, which he believes have little or no apparent correlation to the existing categorization of airports.

One commenter was not comfortable with the difference in the costs of new identification badges at different airports.

FAA response: Since no one can accurately predict the number of airports and how the distribution by size and type for any year in the future, the FAA will not modify these assumptions.

The cost data that the FAA uses is not in one place; instead, it must be gleaned from several different sources. All wage rates were adjusted to 1994 dollars in the NPRM, and 1998 dollars for the Final Rule.

The data gleaned from this analysis applied to GSC's.

The data was obtained from the 1994 survey. Since neither commenter provided different data, the FAA will continue to use the data obtained from the survey.

Since the vast majority are magnetic stripe, cost estimates based on this assumption are expected to be close to the actual amount.

Based on information from industry, the FAA bases its estimate of 1 hour to reissue a card.

According to OMB, the FAA applies a discount factor of 7% to calculate the present value of costs. The GDP implicit price deflators are used to convert costs in different year dollars to the same year dollars.

These airport types track with the security provisions that are in place in the current § 107.3.

The differences in the costs of the badges between the different airports are based in the differences in the wage rates at these airports and in the complexity of the badges needed.

Section 107.3—Definitions

Comments: One commenter believes that the FAA's assertion that changes in definition would not result in any incremental costs is incorrect.

FAA response: This section's purpose is to define the words and terms that will be used later on in the document. When each of these new words and terms are used operationally (in latter sections), they are costed out then.

Section 107.5—Airport Security Coordinator

Comments: One commenter was not comfortable with the FAA's assumption that since the GSC's attrition rate is 5%, the ASC's attrition rate must be the same.

One commenter, in looking at the FAA's costs estimates for additional ASC responsibilities says that the additional ASC duties would need to be transferred to other personnel; the FAA did not cost out the hiring, training, and wages of these additional personnel.

FAA response: Concerning the attrition rates, the commenter offers no other data for the FAA to use, so the FAA will continue to use the 5% attrition rate.

The FAA has no way of knowing if ASC's would need to transfer any of these responsibilities and who they would be reassigned to.

Section 107.9—Falsification

Comments: One commenter does not accept the FAA's belief that there would be few cases that statements or documents would be falsified, and hence, cost would be minor.

FAA response: In the analysis, the FAA specifically invited comments on the number of instances of falsifications that airports have experienced. However, no commenter submitted anything different.

Section 107.11—Security Responsibilities of Persons

Comments: One commenter noted that the FAA assertion that ''the cost of administering a compliance program would only be incurred by airports currently without a program'' was wrong, as existing compliance programs have administrative costs.

One commenter further states that he does not believe that an ASC and a clerk could develop or modify the challenge program in 8 hours.

FAA response: The FAA made a misstatement here and meant to say that ''the *additional* cost of administering a compliance program * * *.''

The FAA agrees with the commenter and is using a figure of 40 hours per each of these employees in the development or modification of the challenge program.

Section 107.103—Content

Comments: Two commenters were not comfortable with the FAA assumption that it would take 15 minutes to assemble each of the elements required by the new section § 107.103.

One commenter believes that the 10-year estimate of $49,200 for administrative costs to change the descriptions in the ASP averages out to $10.69 per airport annually, clearly too low.

FAA response: The FAA agrees and increased the amount of time from 15 to 60 minutes in the final rule analysis.

The FAA is increasing the amount of time required to make these administrative changes, so these costs will rise. In addition, many of the administrative changes will only occur in the first year of implementation.

Section 107.107—Changed Conditions Affecting Security

Comments: One commenter objected to the proposed rule's requirement for airports to report to the FAA any operational changes within a 2-hour period.

Two commenters were confused as to how the FAA's requirement that the Agency be informed of new conditions in 2 hours could lead to cost savings.

FAA response: The FAA has removed the 2-hour time frame from the final rule; the new requirements are that the airport must notify the FAA within 6 hours, or within the time specified in the security program.

The cost savings do not come from these proposed requirements but from new rules that would relieve the airport from formally amending its security program for a condition under 60 days.

Section 107.111—Exclusive Area Agreements

Comments: One commenter does not understand how the FAA's analysis could state that individual costs on the transfer of exclusive use agreements from airports to air carriers will balance out.

FAA response: This analysis looks at any incremental costs. If the airport was doing ''X'' and now the aircraft operator is doing ''X'', to include total aircraft operator costs without looking at total airport savings would be erroneous.

Section 107.201—Security of the Secured Area and Section 107.203—Security of the AOA

Comments: Fourteen commenters make copious arguments against many of the requirements and costs in proposed §§ 107.201 and 107.203. The FAA has modified this section in the final rule, so these comments are not pertinent.

Three commenters believe that adding signage requirements for all doors would increase the cost significantly.

FAA response: If airports change the boundaries of areas to be secured, they will be required to post new signs within these areas. New signs will need to be posted once, not repeatedly and only if the boundaries have been modified.

Section 107.207—Employment History, Verification, and Criminal History Records Checks

Comments: Two commenters questioned the FAA's assertion that it would take $363 to secure a door, as noted in the calculations of proposed § 107.205(f), claiming that the costs of new infrastructure to existing systems would be higher.

One commenter questions whether parts of proposed §§ 107.209 and 107.205 (the NPRM's §§ 107.211 and 107.207) don't contradict each other. He points out that former restricts badge issuance to only 1 per person while the latter allows for the issuance of secondary media.

One commenter was uncomfortable with the FAA's assumption that each employee would forget their access media card on average one time per year.

One commenter objected to the FAA's assertion that employee absences result in supervisors drawing from a labor pool which ensures against employee no-shows; with the exception of reserve flight crews, no airport or air carrier operates with stand-by personnel.

One commenter believes that since there are references to vehicle identification systems in both proposed § 107.205 and in existing part 139, this would lead to two systems that are equally expensive, access control systems.

FAA response: The requirements of proposed § 107.205(f) are not in the final rule. The commenter is confusing the temporary badges discussed by proposed §§ 107.205 (access) and § 107.209 (identification). For the former, the airport may issue a second access media to someone who forgets to bring it to work. For the latter, the airport may issue a second identification media if the employee has more than one job at the airport.

The FAA agrees with the commenter that in the new analysis, the FAA bases costs on the assumption that each employee would forget their access media on average three times a year.

The commenter is correct and such language has been removed from the final rule analysis.

The FAA is not requiring vehicle identification in the final rule.

Section 107.211—Training

Comments: One commenter could not understand the big differences between the costs of personnel and vehicle identification systems.

One commenter believes that applying the challenge procedures to both types of secured areas but having two-tiered training and identification requirements is confusing and costly.

Four commenters believe that having expiration dates on badges, which cause the need to reaudit and revalidate the system, causes great expense and does not augment security.

Six commenters believe that a vehicle identification system would be very expensive.

One commenter objects to an audit that would compare airport records to airline and airport tenant files. Another commenter objected to what it believed was a second yearly audit to compare airport records to airline and airport tenant files.

One commenter could not understand why escort programs ''would not entail costs to airport operators because it codifies a program that is currently in place at all airports in their ASP.''

FAA response: A major reason for this cost differential between personnel and vehicle identification systems is that former involves personnel salary time and picture identification costs; there are no such requirements for vehicle identification. However, the FAA is not requiring vehicle identification in the final rule.

The fact that a challenge system is needed in both areas does not obviate the need to maintain a two-tiered training system.

There are good reasons why an expiration date is needed on identification badges. A person's appearance changes over time. In addition, if an individual losses their identification, anyone would be able to use that badge in the SIDA, perhaps without the picture being carefully viewed by other persons in the area.

Information from the survey indicated that a vehicle identification system at a large airport costs about $4,700 to set up an identification system and $2,300 and $12,100 to audit and revalidate the system, respectively.

The FAA believes that both commenters misread the proposed regulations as there is no such requirement.

Since the FAA is only costing out the new or incremental costs imposed by this proposed regulation, moving a portion of the existing requirements from the ASP to the regulation does not impose any incremental costs.

Section 107.215—Law Enforcement Personnel

Comments: Two commenters were uncomfortable with the FAA using survey data to project cost savings based on the use of plainclothesmen.

FAA response: The FAA has revisited this issue and now believes that there will not be any costing savings.

Section 107.221—Records of Law Enforcement Response

Comments: One commenter notes that the NPRM's § 107.219 (now § 107.221) doubles the requirement for maintaining records, from 90 to 180 days, and wonders why.

FAA response: With regard to the need for 180 days, the FAA stated in the NPRM's Preamble: ''often times, the current 90-day requirement is insufficient for investigation and enforcement purposes.''

Section 107.301—Contingency Plan

Comments: One commenter points out that each airport was required to incorporate the contingency measures into their airport security program several years ago. By shifting this information to the new airport security program, this would involve costs to each airport.

FAA response: The FAA agrees that these contingency measures have existed in each airport operator's security program and believes that they should now be part of the public rule rather than the private rulemaking. In costing out the proposed provisions, the FAA is looking at the incremental change that these changes would impose on the airport. Given that airports already have these contingency provisions, no airport would have to establish one.

Paperwork Reduction Act

Information collection requirements pertaining to this final rule have been approved by the Office of Management and Budget (OMB) for one year under the provisions of the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), and have been assigned OMB control number 2120–0656. Comments

were received on the NPRM publication and are discussed earlier in this preamble.

The FAA is committed to provide the industry with the most current, accurate, and relevant cost impact figures possible. In order not to impede the timely issuance of the regulation, it is our intent to provide updated information on the issues currently contained in the rule, and to solicit additional data from the industry and general public in support of OMB's renewal under the current Paperwork Reduction Act clearance.

The FAA has carefully evaluated the likely incremental burdens of the changes to part 107, and OMB has approved these estimates for a limited period under OMB 2120–0656. However, the FAA recognizes that the rule is codifying many existing practices and procedures, and that the newly codified part 107 will also bring about evolutionary changes of its own. As part of its review of the existing paperwork burden required every 3 years, FAA is now planning a thorough review as part of that renewal clearance of OMB 2120–0075, which expires May 31, 2001. This will also allow the airports and the FAA an opportunity to evaluate how best to implement the changes, and to minimize any new burdens.

It is important to note that the figures contained in the previous clearance for part 107 [OMB #2120–0075], which reflect an estimated annual impact of 75,414 hours of impact, have not changed significantly for a number of years. Those numbers are to a considerable degree based upon long-standing and probably outdated assumptions, and do not fully reflect growth in the demands on airports since that time. Overall traffic at U.S. airports has increased by one-third since 1990, with a concomitant increase in terminal facilities and related demands on security support activities and law enforcement personnel. This includes large demands such as those imposed by the implementation of access controls under § 107.14 in 1989.

During the intervening years, updates of the information collection burden have not kept pace. Amendments have been addressed piecemeal due to periodic security exigencies and legislative requirements. However, a single comprehensive review of the economic impacts of the entire program as an integrated whole has not been possible until this comprehensive rewrite of the regulations. It is our goal to address the informational deficit through additional data gathering and analysis in support of the upcoming May 31, 2001 OMB renewal process.

The current FAA submittal, which estimates approximately 512,000 total annual hours of impact on the industry, must be viewed in a significantly different context from the previous estimates: The FAA will be examining both the old and new regulation in order to validate ongoing burdens and seek to eliminate duplication.

The core provisions of the new regulation have been adopted from current industry practice. Specifically, under the existing regulation, the goals of some security functions are set forth as general mandates. At the same time, the regulation requires the airport operator to accomplish those mandates through language in nonpublic FAA-approved airport security programs. For example, for many years, existing § 107.13 has required airport operators to control access to and movement on certain areas of airports. The implementing details were to be set forth in the security programs. It is the common practice under part 107, to perform this task, in large part, through the use of personal identification (ID) systems. Yet, the existing regulation does not specify the use of such systems; hence, the associated burdens were never adequately reflected. However, the revised part 107 specifically requires the use of ID in certain areas. So, the burdens associated with these systems, while already in place, must be reflected as though totally new. As a result, some of the hours attributed to this new rule are already being expended, so the new burden could actually be less than 512,000 hours. In addition, since the use of such systems has been common industry practice for many years, there exists a considerable amount of industry experience in their implementation. This will allow the FAA to reflect a more valid estimate of impact based on greatly improved data.

Based on extensive comments to the FAA, some costly requirements, such as the access control time and date requirements have been removed from the existing rule, and some NPRM provisions were dropped, such as vehicle IDs and some name changes of the security areas.

Some hours of estimated impact are not really added hours of burden. This regulation simply codifies many existing practices. If anything, the standardization has a strong potential to reduce the collective impact of the rule on both the FAA and the airports.

It is FAA's intent to issue the rule immediately under an interim OMB clearance in order to allow airports to initiate the necessary revisions to their airport security programs. Simultaneously, FAA will initiate the development of an effort to gather updated data to further refine the estimates. These will be submitted to OMB early in 2001 in support of a final clearance under the Paperwork Reduction Act.

As provided for by the Paperwork Reduction Act, it should be noted that 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 Office of Management and Budget (OMB) control number. The assigned control number for the collection of information associated with this rule is 2120–0656.

International Compatibility

In keeping with U.S. obligations under the Convention on International Civil Aviation, it is FAA policy to comply with International Civil Aviation Organization (ICAO) Standards and Recommended Practices to the maximum extent practicable. This proposal is consistent with the ICAO security standards.

Regulatory Evaluation Summary

This rule is considered significant under the regulatory policies and procedures of the Department of Transportation (44 FR 11034; February 26, 1979) but is not considered to have a significant economic impact under Executive Order 12866.

Proposed and final rule changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866 directs that each Federal agency propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980, as amended March 1996, requires agencies to analyze the economic effects of regulatory changes on small entities. Third, OMB directs agencies to assess the effects of regulatory changes on international trade. In conducting these analyses, the FAA has determined that the rule will generate benefits that justify its costs. The rule will not have a significant impact on a substantial number of small entities. The rule will not constitute a barrier to international trade and does not contain Federal intergovernmental or private sector mandates. The full analyses performed in response to the above requirements are contained in the docket and are summarized below.

The FAA analyzed the expected costs of this regulatory proposal for a 10-year period (2000 through 2009). As required by OMB, the present value of this cost stream was calculated using a discount

factor of 7 percent. All costs in this analysis are expressed in 1998 dollars.

The FAA has determined that implementing the final rule changes will affect airport owners; in addition, § 107.307 will impose additional costs on the CASFO representatives.

Currently, there are 458 airports in the U.S. aviation system that have an airport security program approved by the FAA; the contents of these programs, their approval, and the amendment process are key components of part 107. All airport security programs cover many of the same requirements and concerns. However, due to the different physical layouts and security requirements of each airport, each airport's security program will have some unique features. Accordingly, it is important to note there is not a single airport security program, but instead, many programs that have many common elements.

Many of the changes to parts 107 and 139 simply change definitions or make minor word changes. These changes will not result in any incremental costs and will not be covered in this summary. Nine sections will increase costs and two sections will result in cost savings. The changes to security will affect virtually all airports in the system. The analysis assumes no change in the number of airports over the next 10 years.

Section 107.5, entitled ''Airport Security Coordinator'' increases the responsibilities of the ASC. Under this rule, the ASC, or in certain cases the airport operators or their designees, must review materials and security functions for effectiveness and compliance and take corrective action immediately for each instance of non-compliance with this part and notify the FAA of the instances and any corrective measures taken. The ASC must also be trained in accordance with the FAA-approved security program. The estimated cost resulting from these changes total $10.8 million (net present value, $7.6 million).

Section 107.7, entitled, ''Inspection Authority'' (amending the current § 107.27), requires each airport operator to provide the FAA with evidence of compliance with part 107 and its ASP, including copies of records. The airport may be required to send the FAA selected records; for this analysis, the FAA assumes that airports will need to furnish 5% of these reports to the FAA. For this analysis, the FAA assumes that all airports file quarterly. Ten-year costs for these increased records sum to $37,900 (present value, $26,300).

Section 107.103, entitled ''Content'' (amending the current § 107.3) expands the documentation requirements for the airport security programs. The estimated administrative costs will be approximately $420,000 (present value, $330,000).

Section 107.107, entitled ''Changed conditions affecting security'' involves notification costs. All airports are required to notify the FAA to certain changes in airport security. This rule will increase the number of airport security changes of which the FAA needs to be aware and will relieve airports of having to modify their airport security program for a changed security condition under 60 days. The net results of these changes will be an estimated $4.3 million in savings (present value, $3.0 million).

Section 107.201, entitled ''Security of the secured area'' defines the requirements for the most critical security portions of the airport. The intent is to better define the areas of the airport in which the security interest is the most critical and where security measures should be the most stringent. This will entail additional requirements, such as changing warning notices and signs for this area. Most current employees will probably need additional one-time training to educate them as to these new changes. Due to the reclassification and redesignation of the secured area, the FAA believes that 5 percent of all airport employees will no longer need to be issued access media and will no longer need to be trained for access to this area, nor will they need access media. The net result is that these revisions will save an estimated $28.6 million (present value, $15.3 million).

Section 107.203, entitled ''Security of the air operations area'' establishes the means used to control access and movement on the AOA; such access and movement is held to the same standards as controlling access and movement in the secured areas. However, the regulation on the AOA will still entail additional costs including providing information to all employees with access to the AOA and changing warning notices and signs for this area. These revisions will cost an estimated $10.2 million (present value, $9.5 million).

Section 107.207, entitled ''Access control systems'' enhances the existing performance standards for access controls by allowing the issuance of a secondary access medium to individuals. The secondary access media program gives airport operators an option, in addition to using either existing airport escort programs or denying employees access without their original cards, both of which can be very costly. An airport operator opting to use a secondary access media will incur additional costs, including development costs, annual computer time, card manufacturing costs, and card storage costs. A few airports currently escort all employees who do not have their access cards, resulting in lost productivity; costs involved with escorting are covered in § 107.211. Most others deny entry to employees without access cards; they are either sent home to retrieve the card or not allowed to work for the day, so that employee's supervisor needs to spend time reassigning employees. The FAA based its costs by assuming that half the airports adopt the secondary access media and the other half use the current two options. The total 10-year costs for this section total $75.5 million (net present value, $52.7 million).

Section 107.211, entitled ''Identification systems'' requires airports to implement an identification system if they do not have one, and require identification systems to meet certain standards. Such standards will require airports to audit their identification systems once a year and revalidate their identification systems when a certain percentage of the currently issued and active identification media become unaccountable for personnel systems. This section also will require airport operators to implement a challenge program in the secured area and SIDA. The purpose of the challenge program is to improve each airport operator's ability to limit unauthorized incursions in the secured area; the rule requires all airports to make modifications to their present challenge programs. In addition, there will be cost savings from those airports that will no longer use their escort program for employees who forget their access media (as discussed in § 107.207). The total cost of this section will be $7.2 million (present value, $9.2 million).

Section 107.221, entitled ''Records of law enforcement response'' requires that records be maintained pursuant to a schedule in the airport security program and increases the time an airport must maintain records from 90 days to 180 days. Airports will still be required to report all deadly weapon activity, arrests, and threats against civil aviation. The additional recordkeeping and maintenance costs will total $17.8 million (present value, $12.2 million).

Section 107.307, entitled ''Incident management,'' will require that airports incorporate certain procedures into their airport security programs for responding to threats of sabotage, aircraft piracy, and other unlawful acts against civil aviation. This section will also impose

costs upon the FAA; FAA representatives will have to review and approve airport incident threat response procedures and ensure coordination of such procedures with their counterparts in airport safety. Ten-year costs are estimated to be approximately $2.1 million (present value, $1.5 million).

Section 139.325 is amended to require each airport to ensure that the instructions for each airport emergency plan are consistent with its airport security program. This action will entail costs for each airport. The FAA assumes that the ASC and a clerk will each need to spend 2 hours in 2000 and 1 hour in each subsequent year to ensure consistency. Total costs over 10 years equal $270,000 (present value, $200,000).

The 10-year total cost of this rule is estimated to be $92.2 million (present value, $75.4 million).

The rules to amend parts 107 and 108 are intended to enhance aviation safety for U.S. airport operators and aircraft operators in ways that are not currently addressed. The benefits of the rules will be a strengthening of both airport and air carrier security by adding to their effectiveness. Security is achieved through an intricate set of interdependent requirements.

It would be extremely difficult to determine to what extent an averted terrorist incident can be credited to either airport or aircraft security. Accordingly, the benefits from the rules for parts 107 (airport operators) and 108 (aircraft operators) have been combined in this benefit-cost analysis. These benefits are comprised of the criminal and terrorist incidents that these rules are intended to prevent; hence, these benefits will be contrasted against the costs of the changes to parts 107 and 108. The combined costs of part 107 and 108 total $131.3 million (present value, $104.1 million) over 10 years.

Terrorism can occur anytime and anywhere in the United States. Members of foreign terrorist groups, representatives from state sponsors of terrorism, and radical fundamentalist elements from many nations are present in the United States. In addition, Americans are joining terrorist groups. The activities of some of these individuals and groups go beyond fund raising. These activities now include recruiting other persons (both foreign and U.S.) for terrorist activities and training them to use weapons and make bombs. These extremists operate in small groups and can act without guidance or support from state sponsors. This makes it difficult to identify them or to anticipate and counter their activities. The following discussion outlines some of the concrete evidence of the increasing terrorist threat within the United States and to domestic aviation.

Investigation into the February 1993, attack on the World Trade Center (WTC) uncovered a foreign terrorist threat in the United States that is more serious than previously known. The WTC investigation disclosed that Ramzi Yousef had arrived in the United States in September 1992, and had presented himself to immigration officials as an Iraqi dissident-seeking asylum. Yousef and a group of radicals in the United States then spent the next 5 months planning the bombing of the WTC and other acts of terrorism in the United States. Yousef returned to Pakistan on the evening of February 26, 1993, the same day that the WTC bombing took place. By August 1994, Yousef had conceived a plan to bomb as many as 12 U.S. airliners flying between East Asian cities and the United States.

Yousef and his co-conspirators tested the type of explosive devices to be used in the aircraft bombings and demonstrated the group's ability to assemble such a device in a public place, in the December 1994, bombing of a Manila theater. Later the same month, the capability to get an explosive device past airport screening procedures and detonate it aboard an aircraft also was successfully tested when a bomb was placed by Yousef aboard the first leg of Philippine Airlines Flight 424 from Manila to Tokyo. The device detonated during the second leg of the flight, after Yousef had deplaned at an intermediate stop in the Philippine city of Cebu.

Preparations for executing the plan were progressing rapidly. However, the airliner-bombing plot was discovered in January 1995, by chance after a fire led Philippine police to the Manila apartment where the explosive devices were being assembled. Homemade explosives, batteries, timers, electronic components, and a notebook full of instructions for building bombs were discovered. Subsequent investigations of computer files taken from the apartment revealed the plan, in which five terrorists were to have placed explosive devices aboard United, Northwest, and Delta airline flights. It is likely that thousands of passengers would have been killed if the plot had been successfully carried out.

Yousef and his co-conspirators were arrested and convicted in the bombing of Philippine Airlines flight 424 and in the conspiracy to bomb U.S. airliners. Yousef was sentenced to life imprisonment for his role in the Manila plot. Yousef also was convicted and sentenced to 240 years for the WTC bombing. However, there are continuing concerns about the possibility that other conspirators remain at large.

The fact that Ramzi Yousef was responsible for both the WTC bombing and the plot to bomb as many as 12 U.S. air carrier aircraft shows that: (1) Foreign terrorists are able to operate in the U.S. and (2) foreign terrorists are capable of building and artfully concealing improvised explosive devices that pose a serious challenge to aviation security. Civil aviation's prominence as a prospective target is clearly illustrated by the circumstances of the 1995 Yousef conspiracy.

The bombing of a Federal office building in Oklahoma City, Oklahoma, shows the potential for terrorism from domestic groups. While the specific motivation that led to the Oklahoma City bombing would not translate into a threat to civil aviation, the fact that domestic elements have shown a willingness to carry out attacks resulting in indiscriminate destruction is worrisome. At a minimum, the possibility that a future plot hatched by domestic elements could include civil aircraft among possible targets must be taken into consideration. Thus, an increasing threat to civil aviation from both foreign sources and potential domestic ones exists and needs to be prevented and/or countered.

That both the international and domestic threats have increased is undeniable. While it is extremely difficult to quantify this increase in threat, the overall threat can be roughly estimated by recognizing the following:

- U.S. aircraft and American passengers are representatives of the United States, and therefore, are targets;
- Up to 12 airplanes could have been destroyed and thousands of passengers killed in the actual plot described above;
- These plots came close to being carried out; it was only through a fortunate discovery and then extra tight security after the discovery of the plot that these incidents were thwarted;
- It is just as easy for international terrorists to operate within the United States as domestic terrorists, as evidenced by the World Trade Center bombing; therefore,
- Based on these facts, the increased threat to domestic aviation could be seen as equivalent to some portion of 12 Class I Explosions on U.S. airplanes. (The FAA defines Class I Explosions as incidents that involve the loss of an entire aircraft and incur a large number of fatalities.)

In 1996, both Congress and the White House Commission on Aviation Safety

and Security recommended further specific actions to increase civil aviation security. The Commission stated that it believed that the threat against civil aviation was changing and growing, and recommended that the Federal government commit greater resources to improving civil aviation security. President Clinton, in July 1996, declared that the threat of both foreign and domestic terrorism to aviation was a national threat. The U.S. Congress recognized this growing threat in the Federal Aviation Reauthorization Act of 1996 by: (1) authorizing money for the purchase of specific anti-terrorist equipment and the hiring of extra civil aviation security personnel; and (2) requiring the FAA to promulgate additional security-related regulations.

In the absence of increased protection for the U.S. domestic passenger air transportation system, it is conceivable that the system would be targeted for future acts of terrorism. If even one such act were successful, the traveling public would demand immediate increased security. Providing immediate protection on an ad hoc emergency basis would result in major inconveniences, costs, and delays to air travelers that may substantially exceed those imposed by the planned and measured steps contained in these rules.

Based on the above statement, the FAA concludes that these rules set forth a better method to provide increased security at the present time. The FAA considered to the limited extent possible, the benefits of these rules in reducing the costs associated with terrorist acts. The following analysis describes alternative assumptions regarding the number of terrorist acts prevented and potential market disruptions averted that result in these rules' benefits to be at least equal to these rules' costs. This is intended to allow the reader to judge the likelihood of benefits of these rules equaling or exceeding their cost.

The cost of a catastrophic terrorist act can be estimated in terms of lives lost, property damage, decreased public utilization of air transportation, etc. Terrorists acts can result in the complete destruction of an aircraft with the loss of all on board. The FAA considers a Boeing 737 as representative of a typical airplane flown domestically. The fair market value of a Boeing 737 is $16.5 million, and the typical 737 airplane has 113 seats. It flies with an average load factor of 64.7%, which translates into 73 passengers per flight; the airplane will also have 3 pilots and 3 flight attendants.

In order to provide a benchmark comparison of the expected safety benefits of rulemaking actions with estimated costs in dollars; a minimum of $2.7 million is used as the value of avoiding an aviation fatality (based on the willingness to pay approach for avoiding a fatality). In these computations, the present value of each incident was calculated using the current discount rate of 7 percent. Applying this value, the total fatality loss of a single Boeing 737 is represented by a cost $210.6 million (78 × $2.7 million). The safety related costs of a single domestic terrorist act on civil aviation also includes property damage as well as investigative and legal costs, so that the total cost sums to $271.2 million (present value, $190.5 million).

Since the cost of a Class I Explosion on a large domestic airplane is approximately $272 million, coupled with the relative low cost of compliance ($131 million), this rule (and the rule for part 108) will need to prevent one Class I Explosion over the next 10 years in order for quantified benefits to exceed costs. In view of the recent history of terrorist incidents in the United States, a potential catastrophic loss of at least this magnitude is considered to be plausible in the absence of this rule.

The FAA also used the same set of benefits in two proposed rulemakings, *Security of Checked Baggage on Flights Within the United States* and *Certification of Screening Companies.* All of these rulemakings have the same goal—to significantly increase the protection of U.S. citizens and other citizens traveling on U.S. domestic air carrier flights from acts of terrorism as well as increase protection for those operating aircraft. Because the combined discounted costs of all of these rules exceeds $190.9 million, the cost of one Class I Explosion, the FAA calculated the economic impact and the potential averted market disruption sufficient, in combination with safety benefits, to justify all these rulemakings.

Certainly the primary concern of the FAA is preventing loss of life, but there are other considerations as well. Another large economic impact is related to decreased airline travel following a terrorist event. A study performed for the FAA by Pailen-Johnson Associates, Inc., *An Econometric Model of the Impact of Terrorism on U.S. Air Carrier North Atlantic Operations,* indicated that it takes about 9 to 10 months for passenger traffic to return to the pre-incident level after a single event. Such a reduction occurred immediately following the destruction of Pan Am Flight 103 over Lockerbie, Scotland in December 1988. In general, 1988 enplanements were above 1987's. There was a dramatic fall-off in enplanement in the first 3 months of 1989 immediately following the Pan Am 103 tragedy, and it took until November 1989, for enplanements to approximate the 1987 and 1988 levels. Statistics show that there was an almost 20 percent reduction in 1989 in expected enplanements caused by the destruction of Pan Am 103 by terrorists.

The estimated effect of a successful terrorist act on the domestic market has not been studied. Although there are important differences between international and domestic travel (such as the availability of alternative destinations and means of travel), the FAA believes that the traffic loss associated with international terrorist acts is representative of the potential domestic disruption.

There is a social cost associated with travel disruptions and cancellations caused by terrorist events. The cost is composed of several elements. First is the loss associated with passengers opting not to fly—the value of the flight to the passenger (consumer surplus) in the absence of increased security risk and the profit that would be earned by the airline (producer surplus). Even if a passenger opts to travel by air, the additional risk may reduce the associated consumer surplus. Second, passengers who cancel plane trips would not purchase other goods and services normally associated with the trip, such as meals, lodging, and car rental, which would also result in losses of related consumer and producer surplus. Finally, although spending on air travel would decrease, pleasure and business travelers may substitute spending on other goods and services (which produces some value) for the foregone air trips. Economic theory suggests that the sum of the several societal value impacts associated with canceled flights would be a net loss. As a corollary, prevention of market disruption (preservation of consumer and producer welfare) through increased security created by these rules is a benefit.

The FAA is not able to estimate the actual net societal cost of travel disruptions and the corollary benefit gained by preventing the disruptions. However, there is a basis for judging the likelihood of attaining benefits by averting market disruption sufficient, in combination with safety benefits, to justify the rule. The discounted cost of these four rulemakings is $2.3 billion, while the discounted benefits for each Class I Explosion averted comes to $190.9 million. Hence, if one Class I Explosion is averted, the present value of losses due to market disruption must at least equal $2.1 billion ($2.3 billion

less $190.9 million—one Class I Explosion). If two Class I Explosions are averted, the present value of losses due to market disruption must at least equal $1.9 billion ($2.3 billion less $381.8 million—two Class I Explosions).

The value of market loss averted is the product of the number of foregone trips and the average market loss per trip (combination of all impacts on consumer and producer surplus). If one uses an average ticket price of $160 as a surrogate of the combined loss, preservation of a minimum of 13.3 million lost trips would be suffered, in combination with the safety benefits of one averted Class I Explosion, for the benefits of these rulemakings to equal costs. This represents less than 5 percent of annual domestic trips (the traffic loss caused by Pan Am 103 on trans-Atlantic routes was 20 percent). Calculations can be made on the minimum number of averted lost trips needed if the net value loss was only 75 percent of the ticket price or exceeded the ticket price by 25 percent. If total market disruption cost was $130 or $200 per trip, a minimum retention of 16.3 and 10.6 million lost trips, respectively, would need to occur for the benefits to equal the costs of these rulemakings, assuming one Class I Explosion would be prevented. The FAA also calculated the economic impact and the potential averted market disruption sufficient, in combination with safety benefits, to justify all four rulemakings given anywhere from two to four Class I Explosions prevented. These values can be seen in the full economic analysis contained in the docket.

Based on changes in the domestic security risk, the White House Commission recommendation, recent Congressional mandates, and the known reaction of Americans to any air carrier disaster, the FAA believes that pro-active regulation is warranted to prevent terrorist acts (such as Class I Explosions) before they occur.

Final Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980 establishes ''as a principle of regulatory issuance that agencies shall endeavor, consistent with the objective of the rule and of applicable statues, to fit regulatory and informational requirements to the scale of the business, organizations, and governmental jurisdictions subject to regulation.'' To achieve that principle, the Act requires agencies to solicit and consider flexible regulatory proposals and to explain the rational 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 (RFA) 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 act provides that the head of the agency may so certify and an RFA is not required. The certification must include a statement providing the factual basis for this determination, and the reasoning should be clear.

For this rule, the small entity group is considered to be part 107 airports (Standard Industrial Classification Code [SIC] 4581—Airports, Flying Fields, and Airport Terminal Services). The FAA's small entity size standards criterion define a small airport as one owned by a county, city, town, or other jurisdiction having a population of 49,999 or less. If two or more towns, cities, or counties operate an airport jointly, the population size of each is totaled to determine whether that airport is categorized as a small entity. In addition, all privately owned, public-use airports are considered small. The FAA has identified a total of 129 airports that will be considered small entities pursuant to this rule. These 129 airports break down into 31 airports subject to § 107.103(a), 90 airports subject to § 107.103(b), and 8 airports subject to § 107.103(c).

The FAA examined the revenue base for all part 139 small airports. The most reliable measure of income was tax revenues; these averaged out to $2.4 million at the 34th percentile of all small airports subject to part 139. One percent of the 1998 annual revenue for all small airports at the 34th percentile is $24,000 in 1998 dollars. Many part 139 small airports do not have security programs; only those airports that have scheduled service are eligible for such a program. These airports have a larger tax base, greater aviation traffic activity, and overall generate larger tax revenues than airports without scheduled service. Accordingly, the annual tax revenue for airports subject to part 107 is larger than $2.4 million. Moreover, airports with scheduled service earn additional revenues from retail vendor sales, car rental leasing, and fixed-base operator activities. Adding these commercial proceeds to tax revenues boosts the average annual income for these small airports above $2.4 million. Thus, 1 percent of the 1998 annual median revenue for airports impacted by this rule is greater than $24,000 in 1998 dollars.

The FAA has estimated the 10-year and annualized cost impact on each of the small entities. Over 10 years, these regulations will cost each airport subject to §§ 107.103(a), (b), and (c) an estimated $53,000, $34,100, and $31,900, respectively. The annualized costs for these airports are $6,400, $3,400, and $3,200, respectively. These costs are not considered burdensome because they are well below the aforementioned $24,000. Furthermore, as revealed by the above analysis, the revenues and earnings for small airports receiving scheduled traffic is greater than $2.4 million annually. Accordingly, the FAA has determined that the rule will not have a significant economic impact.

Accordingly, pursuant to the Regulatory Flexibility Act, 5 U.S.C. 605(b), the FAA certifies that this rule will not have a significant impact on a substantial number of small entities.

International Trade Impact Statement

In accordance with the OMB memorandum dated March 1983, Federal agencies engaged in rulemaking activities are required to assess the effects of regulatory changes on international trade. This rule will affect all airport owners that have a FAA-approved security program in accord with part 107. Unlike domestic air carriers that compete with foreign air carriers, domestic airports are not in competition with foreign airports. For this reason, a trade impact assessment is not applicable.

Federalism Implications

The FAA has analyzed this final rule under the principles and criteria of Executive Order 13132, Federalism. Most airports subject to this rule are owned, operated, or regulated by a local governmental body (such as a city or county government), which in turn is incorporated by, and derives its authority from, a State. This rule has minimal direct effect on the States, and does not alter the relationship between the airport operators and the FAA that is established in the FAA's statute. The annual costs of compliance with this rule are very low compared with the resources available to the airports. Further, before issuing the NPRM, the FAA consulted with representatives of the airports through the Aviation Security Advisory Committee. Accordingly, the FAA has determined that this action will 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. Therefore, the FAA has determined that this final rule does not have federalism implications.

Unfunded Mandates Reform Act

Title II of the Unfunded Mandates Reform Act of 1995 (the Act), enacted as Pub. L. 104–4 on March 22, 1995, requires each Federal agency, to the extent permitted by law, to prepare a written assessment of the effects of any Federal mandate in a proposed or final agency rule that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any 1 year. Section 204(a) of the Act, 2 U.S.C. 1534(a), requires the Federal agency to develop an effective process to permit timely input by elected officers (or their designees) of State, local, and tribal governments on a proposed ''significant intergovernmental mandate.'' A ''significant intergovernmental mandate'' under the Act is any provision in a Federal agency regulation that will impose an enforceable duty upon State, local, and tribal governments, in the aggregate, of $100 million (adjusted annually for inflation) in any 1 year. Section 203 of the Act, 2 U.S.C. 1533, which supplements section 204(a), provides that before establishing any regulatory requirements that might significantly or uniquely affect small governments, the agency shall have developed a plan that, among other things, provides for notice to potentially affected small governments, if any, and for a meaningful and timely opportunity to provide input in the development of regulatory proposals.

This rule does not contain any Federal intergovernmental mandates or private sector mandates.

Environmental Analysis

FAA Order 1050.1D defines FAA actions that may be categorically excluded from preparation of a National Environmental Policy Act (NEPA) environmental assessment or environmental impact statement. In accordance with FAA Order 1050.1D, appendix 4, paragraph 4(j), this rulemaking action qualifies for a categorical exclusion.

Energy Impact

The energy impact of the notice has been assessed in accordance with the Energy Policy and Conservation Act (EPCA) P.L. 94–163, as amended (43 U.S.C. 6362) and FAA Order 1053.1. It has been determined that the final rule is not a major regulatory action under the provisions of the EPCA.

Distribution/Derivation Tables

The following distribution table is provided to illustrate how the current regulation relates to the revised part 107, and the derivation table identifies how the revised part 107 relates to the current rule.

DISTRIBUTION TABLE

Old section	New section
107.1(a)(1)–(4)	107.1(a)(1)–(4)
107.1(b)(1)–(4)	107.3, which adds eight new unnumbered definitions
107.1(b)(5)	Removed
107.1(b)(6)	Removed
107.2(a)–(c)	107.9(a)–(c)
107.3(a)(1)–(3)	107.101(a)(1)–(3)
107.3(b)	107.103(a)
107.3(b)(1) and (2)	107.103(a)(4)(i)–(ii)
107.3(b)(3)	107.103(a)(20)
107.3(b)(4)	107.103(a)(4)(iii)
107.3(b)(5)	107.111(b)(2)–(3)
107.3(b)(6)	107.103(a)(19)
107.3(b)(7)	107.103(a)(12)
107.3(b)(8)	107.103(a)(11)
107.3(b)(9)	107.103(a)(13)
107.3(c)	107.103(d)
107.3(d) and (e)	107.101(b) and (c)
107.3(f)(1)–(3)	107.103(c)(2)–(4)
107.3(g)(1)–(3)	107.103(b)(2)–(4)
107.5(a)	107.105(a)
107.5(b) and (c)	107.105(a)(1) and (2)
107.5(d) and (e)	107.105(a)(3)
107.7(a)(1)	107.107(a)(3)
107.7(a)(2)	107.107(a)(1)
107.7(a)(3)	107.103(a)(19)
107.7(a)(4)	107.107(b)
107.7(a)(5)	107.107(a)(1)
107.7(b)(1)	107.107(b)(1)
107.7(b)(2)	107.107(c) and (d)
107.9(a) and (b)	107.105(b)(1) and (2)
107.9(c)(1)and (2)	107.105(b)(3)
107.9(d)	107.105(b)(4)
107.9(e) and (f)	107.105(b)(5)
107.11(a)	107.105(c)
107.11(b) and (c)	107.105(c)(1) and (2)
107.11(d) and (e)	107.105(c)(3)
107.11(f)	107.105(d)
107.13(a)	107.203(a)
107.13(a)(1)	107.203(b)(1)
107.13(a)(2)	107.203(b)
107.13(a)(3)	107.203(b)(2)
107.13(b)(1) and (2)	107.111(b)(1)–(3)
107.14(a)	107.207(a)(1)–(3)
107.14(b)	107.207(b)
107.14(c) and (d)	Removed
107.15(a)(1)	107.215(a) and (a)(1)
107.15(a)(2)	107.215(a)(2)
107.15(b)	107.215(b)
107.17(a)–(c)(2)	107.217(a)–(c)(2)
107.17(d)(1)–(4)	107.217(c)(3)(i)–(iv)
107.19	107.219
107.20 and 107.21	Moved to Part 108
107.23(a)	107.221(a)
107.23(a)(2)	107.221(a)(2)
107.23(a)(3)	107.7(b)
107.23(b)	107.221(c)
107.25(a)	107.3
107.25(b) and (e)	107.213(b) and (c)
107.25(c) and (d)	Removed
107.25(e)(1) and (2)	107.213(c)(2) and (3)
107.25(e)(3)–(5)	107.213(c)(5) and (6)
107.25(f)	107.211(a)(3)
107.25(g)	107.213(d)
107.27	107.7(b)
107.29	107.5 (expanded)
107.31	107.209 (unchanged)

DERIVATION TABLE

New section	Old section
107.1(a)(1)–(4)	107.1(a)(1)–(4)
107.1(a)(5)	New
107.1(b)	New
107.3	107.1, plus eight new unnumbered definitions
107.5	107.29
107.5(b)(3)–(6), (c), and (d).	New
107.7, (a), (a)(1) and (2), (c) and (d).	New
107.7(b)	107.27
107.9(a)–(c)	107.2(a)–(c)
107.11(a), (a)(1), (a)(2) and (b).	New
107.101(a)(1)–(3)	107.3(a)(1)–(3)
107.101(a)(4)	New
107.101(a)(5)	107.3(a)(4)
107.101(a)(5)	107.3(a)(4)
107.101(b) and (c)	107.3(d) and (e)
107.103(a)	107.3(b)
107.103(a)(1)	New
107.103(a)(2)	New—Reserved
107.103(a)(3), (a)(3)(i)–(v).	New
107.103(a)(4)(i) and (ii).	107.3(b)(1) and (2)
107.103(a)(4)(iii)	107.3(b)(4)
107.103(a)(11)	107.3(b)(8)
107.103(a)(12)	107.3(b)(7)
107.103(a)(13)	107.3(b)(9)
107.103(a)(14)–(18)	New
107.103(a)(19)	107.3(b)(6)
107.103(a)(20)	107.3(b)(3)
107.103(a)(21)	New
107.103(b)	107.3(g)
107.103(b)(1)	New
107.103(b)(2)–(4)	107.3(g)(1)–(3)
107.103(b)(5)–(8)	New
107.103(c)(1)	New
107.103(c)(2)–(4)	107.3(f)(1)–(3)
107.103(c)(5)–(7)	New
107.103(d)	107.3(c)
107.105(a)	107.5(a)
107.105(a)(1) and (2)	107.5(b) and (c)
107.105(a)(3)	107.5(d) and (e)
107.105(b)(1) and (2)	107.9(a) and (b)
107.105(b)(3)	107.9(c)(1) and (2)
107.105(b)(4)	107.9(d)
107.105(b)(5)	107.9(e) and (f)
107.105(c)	107.11(a)
107.105(c)(1)–(3)	107.11(a), (c) and (d)
107.105(d)	107.11(f)
107.107(a)(1)	107.7(a)(2)

DERIVATION TABLE—Continued

New section	Old section
107.107(a)(2)	New
107.107(a)(3)	107.7(a)(1)
107.107(b)	107.7(b)
107.107(c) and (d)	107.7(b)(2) plus new language
107.109	New
107.111(a)	New
107.111(b) and (b)(1)	107.3(b)(5)
107.111(c)	New
107.113(a)–(d)	New
107.201(a), (b) and (b)(1).	107.14(a)
107.201(b)(2)–(7)	New
107.203(a)	107.13(a)
107.203(b)(1)	107.13(a)(1)
107.203(b)(2)	107.13(a)(3)
107.203(b)(3) and (4)	New
107.205(b)(2) and (3)	New
107.207	107.13 and 107.14
107.207(a)(1)–(3)	107.14(a)
107.207(b)	107.14(b)
107.207(c)(1)–(e)(5)	New
107.209	107.31
107.211(a)(1)(i)–(iv)	New
107.211(a)(3)(i)–(vi),(e).	New
107.213(b) and (c)	107.25(b)–(e)
107.213(b)(1)	New
107.213(b)(2)	107.25(e)(1)
107.213(b)(4)	New
107.213(c)(5) and (6)	107.25(e)(3)–(5)
107.213(c)(1)	New
107.213(c)(2) and (3)	107.25(e)(1) and (2)
107.213(c)(4)	New
107.213(c)(5) and (6)	107.25(e)(3)–(5)
107.213(d)	107.25(g)
107.213(e)	New
107.215(a)	107.15(a)
107.215(a)(1)	107.15(a) and (a)(1)
107.215(a)(2)	107.15(a)(2)
107.215(b)	107.15(b)
107.217(a)–(c)(2)	107.17(a)–(c)(2)
107.217(c)(3)(i)–(iv)	107.17(d)(1)–(4)
107.217(d)	New
107.219	107.19
107.221(a)(1) and (2)	107.23(a)(1) and (2)
107.221(c)	107.23(b)
107.221(d)	New
107.301(a) and (b)	New
107.303(a)–(f)(2)	New
107.305	New
107.307(a)–(d)	New

List of Subjects

14 CFR Part 107

Airports, Arms and munitions, Law enforcement officers, Reporting and recordkeeping requirements, Security measures.

14 CFR Part 139

Air carriers, Airports, Aviation safety.

The Amendments

In consideration of the foregoing, the Federal Aviation Administration amends chapter I of Title 14, Code of Federal Regulations as follows:

1. Part 107 is revised to read as follows:

PART 107—AIRPORT SECURITY

Subpart A—General

Subpart B—Airport Security Program

Subpart C—Operations

Subpart D—Contingency Measures

Authority: 49 U.S.C. 106(g), 5103, 40113, 40119, 44701–44702, 44706, 44901–44905, 44907, 44913–44914, 44932, 44935–44936, 46105.

Subpart A—General

§ 107.1 Applicability.

(a) This part describes aviation security rules governing:

(1) The operation of each airport regularly serving aircraft operations required to be under a security program under part 108 of this chapter.

(2) The operation of each airport regularly serving foreign air carrier operations required to be under a security program under § 129.25 of this chapter.

(3) Each person who is in, or entering, a secured area, air operations area, security identification display area, or sterile area described in this part and part 108 of this chapter.

(4) Each person who files an application or makes entries into any record or report that is kept, made, or used to show compliance under this part, or to exercise any privileges under this part.

(5) 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 Assistant Administrator for Civil Aviation Security.

(b) Except as provided in § 107.105, the authority of the Administrator under this part is also exercised by the Assistant Administrator for Civil Aviation Security and the Deputy Assistant Administrator for Civil Aviation Security, and any individual formally designated to act in their capacity. The authority of the Assistant Administrator, including matters under § 107.105, may be further delegated.

§ 107.3 Definitions.

Terms defined in part 108 of this chapter apply to this part. For purposes of this part, part 108 of this chapter, and security programs under these parts, the following definitions also apply:

Air operations area (AOA) means a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas, for use by aircraft regulated under part 108 or § 129.25 of this chapter, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the secured area.

Airport operator means a person that operates an airport serving an aircraft operator or a foreign air carrier required to have a security program under part 108 or § 129.25 of this chapter.

Airport security program means an airport operator's security program required under § 107.101 and approved by the Administrator.

Airport tenant means any person, other than an aircraft operator or foreign air carrier that has a security program under part 108 or § 129.25 of this chapter, that has an agreement with the airport operator to conduct business on airport property.

Airport tenant security program means the agreement between the airport operator and an airport tenant that specifies the measures by which the tenant will perform security functions under § 107.113.

Assistant Administrator means the FAA Assistant Administrator for Civil Aviation Security as described in 49 U.S.C. 44932.

Escort means to accompany or monitor the activities of an individual

who does not have unescorted access authority into or within a secured area or SIDA.

Exclusive area means any portion of a secured area, AOA, or SIDA, including individual access points, for which an aircraft operator or foreign air carrier that has a security program under part 108 or § 129.25 of this chapter has assumed responsibility under § 107.111.

Exclusive area agreement means an agreement between the airport operator and an aircraft operator or a foreign air carrier that has a security program under part 108 or § 129.25 of this chapter that permits such an aircraft operator or foreign air carrier to assume responsibility for specified security measures in accordance with § 107.111.

Secured area means a portion of an airport, specified in the airport security program, in which certain security measures specified in this part are carried out. This area is where aircraft operators and foreign air carriers that have a security program under part 108 or § 129.25 of this chapter enplane and deplane passengers and sort and load baggage and any adjacent areas that are not separated by adequate security systems, measures, or procedures.

Security Identification Display Area (SIDA) means a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.

Unescorted access authority means the authority granted to individuals by an airport operator, aircraft operator, foreign air carrier, or airport tenant authorized under this part or parts 108 or 129 of this chapter to gain entry to, and be present without an escort in secured areas and SIDA's.

§ 107.5 Airport security coordinator.

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

(b) The airport operator shall ensure that one or more ASC's:

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

(2) Is available to the Administrator 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 § 107.209.

(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 shall maintain ASC training documentation until at least 180 days after the withdrawal of a 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.

§ 107.7 Inspection authority.

(a) For purposes of security inspections, each airport operator shall allow Special Agents designated by the Administrator, 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 part, parts 108, 109, 129, and 191 of this chapter and any security program approved under those parts; and

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

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

(c) The Administrator 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 conduct investigations, inspect, test compliance, or perform other such duties as the Administrator may direct.

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

§ 107.9 Falsification.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any application for any security program, access medium, or identification medium, or any amendment thereto, under this part.

(b) Any fraudulent or intentionally false entry in any record or report that is kept, made, or used to show compliance with this part, or exercise any privileges under this part.

(c) Any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access medium, or identification medium issued under this part.

§ 107.11 Security responsibilities of employees and other persons.

(a) No person may:

(1) Tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under this part.

(2) Enter, or be present within, a secured area, AOA, SIDA or sterile area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas.

(3) Use, allow to be used, or cause to be used, any airport-issued or airport-approved access medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in secured areas, AOA's, or SIDA's in any other manner than that for which it was issued by the appropriate authority under this part, or part 108 or part 129 of this chapter.

(b) The provisions of paragraph (a) of this section do not apply to conducting inspections or tests to determine compliance with this part or 49 U.S.C. Subtitle VII authorized by:

(1) The Administrator, or

(2) The airport operator, aircraft operator, or foreign air carrier, when acting in accordance with the procedures described in a security program approved by the Administrator.

Subpart B—Airport Security Program

§ 107.101 General requirements.

(a) No person may operate an airport subject to this part 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 deadly or dangerous weapon, explosive, or incendiary onto an aircraft;

(2) Is in writing and is signed by the airport operator or any person to whom the airport operator has delegated authority in this matter;

(3) Includes the applicable items listed in § 107.103;

(4) Includes an index organized in the same subject area sequence as § 107.103; and

(5) Has been approved by the Administrator.

(b) The airport operator shall maintain one current and complete copy of its security program and provide a copy to the Administrator upon request.

(c) Each airport operator shall—

(1) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 191 of this chapter, to persons with a need to know; and

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

§ 107.103 Content.

(a) Except as otherwise approved by the Administrator, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in §§ 108.101(a)(1) or 129.25(b)(1) of this chapter, shall include in its security program the following:

(1) The name, means of contact, duties, and training requirements of the ASC required under § 107.5.

(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) Systems, measures, and procedures used to perform the access control functions required under § 107.201(b)(1);

(iv) Procedures to control movement within the secured area, including identification media required under § 107.201(b)(3); and

(v) A description of the notification signs required under § 107.201(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) Systems, measures, and procedures used to perform the access control functions required under § 107.203(b)(1);

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

(v) A description of the notification signs required under § 107.203(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) Systems, measures, and procedures used to control access as specified in § 107.207.

(7) Procedures used to comply with § 107.209 regarding employment history, verification, and criminal history records checks.

(8) A description of the personnel identification systems as described in § 107.211.

(9) Escort procedures in accordance with § 107.211(e).

(10) Challenge procedures in accordance with § 107.211(d).

(11) Training programs required under §§ 107.213 and 107.217(c)(2), if applicable.

(12) A description of law enforcement support used to comply with § 107.215(a).

(13) A system for maintaining the records described in § 107.221.

(14) The procedures and a description of facilities and equipment used to support aircraft operator or foreign air carrier screening functions of §§ 108.201 or 129.25 of this chapter.

(15) A contingency plan required under § 107.301.

(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 § 107.305.

(18) Incident management procedures used to comply with § 107.307.

(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 § 107.111.

(21) Each airport tenant security program as specified in § 107.113.

(b) Except as otherwise approved by the Administrator, each airport regularly serving operations of an aircraft operator or foreign air carrier described in §§ 108.101(a)(2) or (b), or 129.25(b)(2) or (b)(3) of this chapter, shall 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 § 107.5.

(2) A description of the law enforcement support used to comply with § 107.215(a).

(3) Training program for law enforcement personnel required under § 107.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 107.221.

(5) The contingency plan required under § 107.301.

(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 § 107.305.

(8) Incident management procedures used to comply with § 107.307.

(c) Except as otherwise approved by the Administrator, each airport regularly serving operations of an aircraft operator or foreign air carrier described in §§ 108.101(c) or 129.25(b)(4) of this chapter, shall 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 § 107.5.

(2) A description of the law enforcement support used to comply with § 107.215(b).

(3) Training program for law enforcement personnel required under § 107.217(c)(2), if applicable.

(4) A system for maintaining the records described in § 107.221.

(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 § 107.305.

(7) Incident management procedures used to comply with § 107.307.

(d) 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 shall be referenced in the corresponding section(s) of the security program.

§ 107.105 Approval and amendments.

(a) *Initial approval of security program.* Unless otherwise authorized by the Assistant Administrator, each airport operator required to have a security program under this part shall submit its initial proposed security program to the Assistant Administrator for approval at least 90 days before the date any aircraft operator or foreign air carrier required to have a security program under §§ 108.101 or 129.25 of this chapter is expected to begin operations. Such requests will be processed as follows:

(1) The Assistant Administrator, 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 Assistant Administrator 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 Assistant Administrator.

(3) The Assistant Administrator, 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 Assistant Administrator 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 § 107.107(c), an airport operator may submit a request to the Assistant Administrator to amend its security program, as follows:

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

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

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

(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 Assistant Administrator 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 Assistant Administrator to approve the amendment or affirm the denial.

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

(1) The Assistant Administrator 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 Assistant Administrator 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 shall send the petition for reconsideration to the Assistant Administrator. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the Assistant Administrator 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 Assistant Administrator to withdraw or amend the amendment, or by affirming the amendment.

(d) *Emergency Amendments.* Notwithstanding paragraph (c) of this section, if the Assistant Administrator 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 Assistant Administrator may issue an amendment, effective without stay on the date the airport operator receives the notice of it. In such a case, the Assistant Administrator shall 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 (EA).

§ 107.107 Changed conditions affecting security.

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

(1) Systems, measures, procedures, 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 § 107.103; 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 parts 107, 108, or 129 of this chapter.

(b) Each airport operator shall notify the Administrator 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 shall inform the Administrator 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 the Administrator.

(c) For changed conditions expected to be less than 60 days duration, each airport operator shall forward the information required in paragraph (b) of this section in writing to the Administrator within 72 hours of the original notification of the change condition(s). The Administrator will notify the airport operator of the disposition of the notification in writing. If approved by the Administrator, 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 shall 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 § 107.105. The request for an amendment shall be made within 30

days of the discovery of the changed condition(s). The Administrator will respond to the request in accordance with § 107.105.

§ 107.109 Alternate means of compliance.

If in the Administrator's judgment, the overall safety and security of the airport, and aircraft operator or foreign air carrier operations are not diminished, the Administrator 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 §§ 108.101 or 129.25 of this chapter is determined by the Administrator to be seasonal or infrequent.

§ 107.111 Exclusive area agreements.

(a) The Administrator 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 108 or part 129 of this chapter assumes responsibility for specified security measures for all or portions of the secured area, AOA, or SIDA, as provided in §§ 107.201, 107.203, or 107.205. 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 shall be in writing, signed by the airport operator and aircraft operator or foreign air carrier, and maintained in the airport security program. This agreement shall 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 systems, measures, and procedures used by the aircraft operator or foreign air carrier to comply with §§ 107.201, 107.203, or 107.205, 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 § 107.107(a).

(c) Any exclusive area agreements in effect on November 14, 2001 shall meet the requirements of this section and § 108.227 no later than November 14, 2002.

§ 107.113 Airport tenant security programs.

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

(1) The tenant must assume responsibility for specified security systems, measures, or procedures of the secured area, AOA, or SIDA as provided in §§ 107.201, 107.203, and 107.205.

(2) The tenant may only assume responsibility for employment verification as provided in § 107.209.

(3) The tenant may not assume responsibility for law enforcement support under § 107.215.

(4) 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.

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

(6) The Administrator must find that the tenant is able and willing to carry out the airport tenant security program.

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

(1) A description and a map of the boundaries and pertinent features of each area over which the airport tenant will exercise security responsibilities.

(2) A description of the systems, measures, and procedures the airport tenant has assumed.

(3) Systems, measures, and procedures 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 the Administrator in accordance with § 107.7.

(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 191 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 § 107.107(a).

(c) If the Administrator 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) The Administrator may amend or terminate an airport tenant security program in accordance with § 107.105.

Subpart C—Operations

§ 107.201 Security of the secured area.

(a) Each airport operator required to have a security program under § 107.103(a) shall establish at least one secured area.

(b) Each airport operator required to establish a secured area shall 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 systems, measures, or procedures for controlling entry to secured areas 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 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 § 107.211.

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

(5) Train each individual before granting unescorted access to the secured area, as required in § 107.213(b).

(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 Employment history, verification, and criminal history records checks.

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

(1) All airport operators, airport users, and individuals currently having unescorted access to a SIDA.

(2) All individuals seeking authorization for, or seeking the authority to authorize others to have, unescorted access to the SIDA.

(3) Each airport user and aircraft operator making a certification to an airport operator pursuant to paragraph (n) of this section, made on or after January 31, 1996. An airport user, for the purposes of this section only, is any person making a certification under this section other than an aircraft operator subject to § 108.229 of this chapter.

(b) *Employment history investigations required.* Except as provided in paragraph (m) of this section, each airport operator must ensure that no individual is granted authorization for, or is granted authority to authorize others to have, unescorted access to the SIDA unless the following requirements are met:

(1) The individual has satisfactorily undergone Part 1 of an employment history investigation. Part 1 consists of a review of the previous 10 years of employment history and verification of the 5 employment years preceding the date the appropriate investigation is initiated as provided in paragraph (c) of this section; and

(2) If required by paragraph (c)(5) of this section, the individual must then satisfy Part 2 of the employment history investigation. Part 2 is the process to determine if the individual has a criminal record. To satisfy Part 2 of the investigation the criminal record check must not disclose that the individual has been convicted or found not guilty by reason of insanity, in any jurisdiction, during the 10 years ending on the date of such investigation, of any of the crimes listed as follows:

(i) Forgery of certificates, false marking of aircraft, and other aircraft registration violation, 49 U.S.C. 46306;

(ii) Interference with air navigation, 49 U.S.C. 46308;

(iii) Improper transportation of a hazardous material, 49 U.S.C. 46312;

(iv) Aircraft piracy, 49 U.S.C. 46502;

(v) Interference with flightcrew members or flight attendants, 49 U.S.C. 46504;

(vi) Commission of certain crimes aboard aircraft in flight, 49 U.S.C. 46506;

(vii) Carrying a weapon or explosive aboard aircraft, 49 U.S.C. 46505;

(viii) Conveying false information and threats, 49 U.S.C. 49 46507;

(ix) Aircraft piracy outside the special aircraft jurisdiction of the United States, 49 U.S.C. 46502(b);

(x) Lighting violations involving transporting controlled substances, 49 U.S.C. 46315;

(xi) 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;

(xii) Destruction of an aircraft or aircraft facility, 18 U.S.C. 32;

(xiii) Murder;

(xiv) Assault with intent to murder;
(xv) Espionage;
(xvi) Sedition;
(xvii) Kidnapping or hostage taking;
(xviii) Treason;
(xix) Rape or aggravated sexual abuse;
(xx) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon;
(xxi) Extortion;
(xxii) Armed robbery;
(xxiii) Distribution of, or intent to distribute, a controlled substance;
(xxiv) Felony arson; or
(xxv) Conspiracy or attempt to commit any of the aforementioned criminal acts; and

(3) If an individual admits to a conviction, or to having been found not guilty by reason of insanity, in any jurisdiction within the preceding 10 years of a crime listed in (b)(2) of this section, the investigative process shall end and the individual shall not be granted unescorted access or assigned to any functions listed in (a)(3) of this section.

(c) *Investigative steps.* Part 1 of the employment history investigation must be completed on all persons listed in paragraph (a) of this section. If required by paragraph (c)(5) of this section, Part 2 of the employment history investigation must also be completed on all persons listed in paragraph (a) of this section.

(1) The individual must provide the following information on an application form:

(i) The individual's full name, including any aliases or nicknames.

(ii) The dates, names, phone numbers, and addresses of previous employers, with explanations for any gaps in employment of more than 12 consecutive months, during the previous 10-year period.

(iii) Any convictions during the previous 10-year period of the crimes listed in paragraph (b)(2) of this section.

(2) The airport operator or the airport user must include on the application form a notification that the individual will be subject to an employment history verification and possibly a criminal records check.

(3) The airport operator or the airport user must verify the identity of the individual through the presentation of two forms of identification, one of which must bear the individual's photograph.

(4) The airport operator or the airport user must verify the information on the most recent 5 years of employment history required under paragraph (c)(1)(ii) of this section. Information must be verified in writing, by documentation, by telephone, or in person.

(5) If one or more of the conditions (triggers) listed in paragraphs (c)(5)(i) through (c)(5)(iv) of this section exist, the employment history investigation must not be considered complete unless Part 2 is accomplished. Only the airport operator may initiate Part 2 for airport users under this section. Part 2 consists of a comparison of the individual's fingerprints against the fingerprint files of known criminals maintained by the Federal Bureau of Investigation (FBI). The comparison of the individual's fingerprints must be processed through the FAA. The airport operator may request a check of the individual's fingerprint-based criminal record only if one or more of the following conditions exist:

(i) The individual does not satisfactorily account for a period of unemployment of 12 consecutive months or more during the previous 10-year period.

(ii) The individual is unable to support statements made on the application form.

(iii) There are significant inconsistencies in the information provided on the application.

(iv) Information becomes available to the airport operator or the airport user during the investigation indicating a possible conviction for one of the crimes listed in paragraph (b)(2) of this section.

(d) *Individual notification.* Prior to commencing the criminal records check, the airport operator must notify the affected individual and identify the ASC as a contact for follow-up. An individual, who chooses not to submit fingerprints, after having met a requirement for Part 2 of the employment investigation, may not be granted unescorted access privilege.

(e) *Fingerprint processing.* If a fingerprint comparison is necessary under paragraph (c)(5) of this section to complete the employment history investigation the airport operator must collect and process fingerprints in the following manner:

(1) One set of legible and classifiable fingerprints must be recorded on fingerprint cards approved by the FBI, and distributed by the FAA for this purpose.

(2) The fingerprints must be obtained from the individual under direct observation by the airport operator or a law enforcement officer. Individuals submitting their fingerprints may not take possession of their fingerprint card after they have been fingerprinted.

(3) The identity of the individual must be verified at the time fingerprints are obtained. The individual must present two forms of identification, one of which must bear the individual's photograph.

(4) The fingerprint card must be forwarded to the FAA at the location specified by the Administrator.

(5) Fees for the processing of the criminal record checks are due upon application. Airport operators must submit payment through corporate check, cashier's check, or money order made payable to ''U.S. FAA,'' at the designated rate for each fingerprint card. Combined payment for multiple applications is acceptable. The designated rate for processing the fingerprint cards is available from the local FAA security office.

(f) *Determination of arrest status.* In conducting the criminal record checks required by this section, the airport operator must not consider the employment history investigation complete unless it investigates arrest information for the crimes listed in paragraph (b)(2) of this section for which no disposition has been recorded and makes a determination that the arrest did not result in a disqualifying conviction.

(g) *Availability and correction of FBI records and notification of disqualification.* (1) At the time Part 2 is initiated and the fingerprints are collected, the airport operator must notify the individual that a copy of the criminal record received from the FBI will be made available to the individual if requested in writing. When requested in writing, the airport operator must make available to the individual a copy of any criminal record received from the FBI.

(2) Prior to making a final decision to deny authorization to an individual described in paragraph (a) of this section, the airport operator must advise the individual that the FBI criminal record discloses information that would disqualify him/her from receiving unescorted access and provide the individual with a copy of the FBI record if it has been requested.

(3) The airport operator must notify an individual that a final decision has been made to grant or deny authority for unescorted access.

(h) *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/her record before any final decision is made, subject to the following conditions:

(1) Within 30 days after being advised that the criminal record received from the FBI discloses disqualifying information, the individual must notify the airport operator, in writing, of his/

her intent to correct any information believed to be inaccurate.

(i) Upon notification by an individual that the record has been corrected, the airport operator must obtain a copy of the revised FBI record prior to making a final determination.

(ii) [Reserved]

(2) If no notification is received within 30 days, the airport operator may make a final determination.

(i) *Limits on dissemination of results.* Criminal record information provided by the FBI must be used solely for the purposes of this section, and no person may disseminate the results of a criminal record check to anyone other than:

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

(2) Airport officials with a need to know; and

(3) Others designated by the Administrator.

(j) *Employment status while awaiting criminal record checks.* Individuals who have submitted their fingerprints and are awaiting FBI results may perform work within the SIDA when under escort by someone who has unescorted SIDA access privileges.

(k) *Recordkeeping.* (1) Except when the airport operator has received a certification under paragraph (n)(1) of this section, the airport operator must physically maintain and control the Part 1 employment history investigation file until 180 days after the termination of the individual's authority for unescorted access. The Part 1, employment history investigation file, must consist of the following:

(i) The application;

(ii) The employment verification information obtained by the employer;

(iii) The names of those from whom the employment verification information was obtained;

(iv) The date and the method of how the contact was made; and

(v) Any other information as required by the Administrator.

(2) The airport operator must physically maintain, control and when appropriate destroy Part 2, the criminal record, for each individual for whom a fingerprint comparison has been completed. Part 2 must be maintained for 180 days after the termination of the individual's authority for unescorted access. Only direct airport operator employees may carry out this criminal record file responsibility. The Part 2 criminal record file must consist of the following:

(i) The criminal record received from the FBI as a result of an individual's fingerprint comparison; or

(ii) Information that the check was completed and no record exists.

(3) The files required by this section must be maintained in a manner that is acceptable to the Administrator and in a manner that protects the confidentiality of the individual.

(l) *Continuing responsibilities.* (1) Any individual authorized to have unescorted access privileges or who may authorize others to have unescorted access, who is subsequently convicted of any of the crimes listed in paragraph (b)(2) of this section must, within 24 hours, report the conviction to the airport operator and surrender the SIDA access medium to the issuer.

(2) If information becomes available to the airport operator or the airport user indicating that an individual with unescorted access has a possible conviction for one of the disqualifying crimes in paragraph (b)(2) of this section, the airport operator must determine the status of the conviction. If a disqualifying conviction is confirmed the airport operator must withdraw any authority granted under this section.

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

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

(2) A crewmember of a foreign air carrier covered by an alternate security arrangement in the foreign air carrier's approved security program.

(3) An individual who has been continuously employed in a position requiring unescorted access by another airport operator, airport user or aircraft operator.

(4) Those persons who have received access to a U.S. Customs secured area prior to November 24, 1998.

(n) *Investigations by aircraft operators and airport users.* An airport operator is in compliance with its obligation under paragraph (b) of this section, as applicable, when the airport operator accepts for each individual seeking unescorted access one of the following:

(1) Certification from an aircraft operator subject to § 108.229 of this chapter indicating it has complied with § 108.229 of this chapter for the aircraft operator's employees and contractors seeking unescorted access; or

(2) Certification from an airport user indicating it has complied with and will continue to comply with the provisions listed in paragraph (p) of this section. The certification must include the name of each individual for whom the airport user has conducted an employment history investigation.

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

(1) Prior to the acceptance of a certification from the airport user, the airport operator must conduct a preliminary review of the file for each individual listed on the certification to determine that Part 1 has been completed;

(2) Designate the ASC, in the security program, to be responsible for reviewing the results of the airport employees' and airport users' employment history investigations and for destroying the criminal record files when their maintenance is no longer required by paragraph (k)(2) of this section;

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

(4) Audit the employment history investigations performed by the airport operator in accordance with this section and those investigations conducted by the airport users made by certification under paragraph (n)(2) of this section. The audit program must be set forth in the airport security program.

(p) *Airport user responsibility.* (1) The airport user is responsible for reporting to the airport operator information, as it becomes available, which indicates an individual with unescorted access may have a conviction for one of the disqualifying crimes in paragraph (b)(2) of this section.

(2) If the airport user offers certification to the airport operator under paragraph (n)(2) of this section, the airport user must for each individual for whom a certification is made:

(i) Conduct the employment history investigation, Part 1, in compliance with paragraph (c) of this section. The airport user must report to the airport operator if one of the conditions in paragraph (c)(5) of this section exist;

(ii) Maintain and control Part 1 of the employment history investigation file in compliance with paragraph (k) of this section, unless the airport operator decides to maintain and control Part 1 of the employment history investigation file;

(iii) Provide the airport operator and the FAA with access to each completed Part 1 employee history investigative

file of those individuals listed on the certification; and

(iv) Provide either the name or title of the individual acting as custodian of the files, and the address of the location and the phone number at the location where the investigative files are maintained.

§ 107.211 Identification systems.

(a) *Personnel identification system.* The personnel identification system under §§ 107.201(b)(3) and 107.205(b)(1) shall 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 shall 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 § 107.207(d).

(c) *Airport-approved identification media.* The Administrator 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 shall 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 shall include procedures to challenge individuals not displaying airport approved identification media. The procedure must—

(1) Apply uniformly in secured areas, SIDAs, 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 shall 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 § 108.201 of this chapter remain under escort until they exit the sterile area, or submit to screening pursuant to § 108.201 or part 129 of this chapter.

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

§ 107.213 Training.

(a) Each airport operator shall 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.

(b) An airport operator may not authorize any individual unescorted access to the secured area or SIDA, except as provided in § 107.7, unless that individual has successfully completed training in accordance with the FAA-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 § 107.11;

(5) Restrictions on divulging sensitive security information as described in part 191 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 § 107.7, 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 § 107.11;

(5) Restrictions on divulging sensitive security information as described in part 191 of this chapter; and

(6) Any other topics specified in the security program.

(d) Each airport operator shall 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, training on responsibility under § 107.11 can be provided by making relevant security information available.

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

§ 107.215 Law enforcement support.

(a) In accordance with § 107.217, each airport operator required to have a security program under § 107.103(a) or (b) shall 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 § § 108.201 or 129.25 of this chapter.

(b) Each airport required to have a security program under § 107.103(c) shall 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 108 or § 129.25 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 108 or § 129.25 of this chapter.

§ 107.217 Law enforcement personnel.

(a) Each airport operator shall ensure that law enforcement personnel used to meet the requirements of § 107.215, 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 shall ensure that each individual used to meet the requirements of § 107.215 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 shall—

(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 the Administrator, 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 the Administrator determines is necessary.

(d) Each airport operator shall 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.

§ 107.219 Supplementing law enforcement personnel.

(a) When the Administrator 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 § 107.215, the Administrator may authorize the airport operator to use, on a reimbursable basis, personnel employed by the Administrator, 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 the Administrator 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 § 107.215.

(4) The availability of law enforcement personnel who meet the requirements of § 107.217, 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 the Administrator considers necessary.

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

§ 107.221 Records of law enforcement response.

(a) Each airport operator shall 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:

(1) The number and type of deadly or dangerous weapon, 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 deadly or dangerous 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

§ 107.301 Contingency plan.

(a) Each airport operator required to have a security program under § 107.103(a) and (b) shall adopt a contingency plan and shall:

(1) Implement its contingency plan when directed by the Administrator.

(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) The Administrator 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 107.301(a).

§ 107.303 Security Directives and Information Circulars.

(a) The Administrator may issue an Information Circular to notify airport operators of security concerns. When the Administrator determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, the Administrator issues a Security Directive setting forth mandatory measures.

(b) Each airport operator shall 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 shall—

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

(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 shall submit proposed alternative measures and the basis for submitting the alternative measures to the Administrator for approval. The airport operator shall submit the proposed alternative measures within the time prescribed in the Security Directive. The airport operator shall implement any alternative measures approved by the Administrator.

(e) Each airport operator that receives a Security Directive may comment on the Security Directive by submitting data, views, or arguments in writing to the Administrator. The Administrator 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 shall:

(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 the Administrator.

§ 107.305 Public advisories.

When advised by the Administrator, each airport operator shall 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 shall be posted in the manner specified in the security program and for such a period of time determined by the Secretary of Transportation.

§ 107.307 Incident management.

(a) Each airport operator shall 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 shall—

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

(2) Initiate appropriate action as specified in the Airport Emergency Plan under § 139.325 of this chapter; and

(3) Immediately notify the Administrator 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 § 107.103(c) but not subject to part 139 of this chapter, shall 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 shall review the procedures required in paragraphs (a) and (b) of this section with all persons having responsibilities for such procedures.

PART 139—CERTIFICATION AND OPERATIONS: LAND AIRPORTS SERVING CERTAIN AIR CARRIERS

2. The authority citation for part 139 continues to read as follows:

Authority: 49 U.S.C. 106 (g), 40113, 44701–44706, 44709, 44719.

3. Section 139.325 is amended by redesignating paragraph (h) as paragraph (i) and adding new paragraph (h) to read as follows:

§ 139.325 Airport emergency plan.

* * * * *

(h) Each airport subject to part 107 of this chapter, Airport Security, shall ensure that instructions for response to paragraphs (b)(2) and (b)(6) of this section in the airport emergency plan are consistent with its approved security program.

* * * * *

Issued in Washington, DC, on July 2, 2001.

Jane F. Garvey,

Administrator.

[FR Doc. 01–16994 Filed 7–10–01; 10:32 am]

BILLING CODE 4910–13–P