DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 107, 108, 109, 129, 191

[Docket No. 27965; Amendment Nos. 107–10, 108–15, 109–3, 129–26, and 191–4]

RIN 2120–AF49

Sensitive Security Information

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This final rule strengthens the existing rules protecting sensitive security information from unauthorized disclosure. Part 191 is expanded to apply to air carriers, airport operators, indirect air carriers, foreign air carriers, and individuals, and specifies in more detail what sensitive security information they must protect. Part 191 continues to describe what information is protected from disclosure by the FAA, and describes in more detail that information. This final rule also changes part 107, 108, 109, and 129 to correspond with changes it makes to part 1991. This action is necessary to counter the increased sophistication of those who pose a threat to civil aviation and their ability to develop techniques to subvert current security measures. The intended effect of this action is to prevent undue disclosure of information that could compromise public safety if it falls into the wrong hands, while being mindful of the public's legitimate right to know and interest in aviation information.

DATES: This rule is effective April 21, 1997. FAA will comply with the provisions of this rule on March 21, 1997.

FOR FURTHER INFORMATION CONTACT: Robert S. Cammardto, Office of Civil Aviation Security Division, ACP–100, Office of Civil Aviation Security Policy and Planning, Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591; telephone (202) 267–7723.

SUPPLEMENTARY INFORMATION:

Background

The Security Regulatory Scheme

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 carry out the provisions of the statute, the FAA has adopted rules requiring airport operators, air carriers, indirect air carriers, and foreign air carriers to carry out various duties for civil aviation security. Title 14, Code of Federal Regulations, part 107 (14 CFR part 107) applies to certain airport operators. Part 108 (14 CFR part 108) governs certain air carriers.

Part 109 (14 CFR part 109) applies to indirect air carriers such as freight forwarders, who engage indirectly in air transportation of property. Part 129 (14 CFR part 129) applies to the operation of foreign air carriers within the United States.

Parts 107, 108, 109, and 129 contain general requirements for promoting civil aviation security. Each airport operator, air carrier, indirect air carrier, and foreign air carrier covered by these parts also has a security program that is approved or accepted by the Administrator, containing information that specifies how airport operators and air carriers perform their regulatory and statutory responsibilities. These security programs are available only to persons with the need-to-know, as described more fully below.

Each air carrier's security program is a comprehensive document that details the full range of security procedures and countermeasures that air carriers are required to perform under 14 CFR 108.5. This program includes procedures for: (1) Screening of passengers, carry-on baggage, checked baggage, and cargo; (2) using screening devices (such as X-ray systems and metal detectors); (3) controlling access to aircraft and air carrier facilities; (4) reporting and responding to bomb threats, hijackings, and weapons discovered during screening; (5) reporting and protecting bomb threat information; (6) identifying special procedures required at airports with special security needs; and (7) training and testing standards for crewmembers and security personnel.

The airport security program is a comprehensive document that details the full range of security procedures and countermeasures that airport operators are required to perform under 14 CFR 107.3. Most programs include: (1) Descriptions of the air operations area (AOA), each area on or adjacent to the airport that affect the security of the AOA, and air carriers exclusive areas; (2) procedures to control access to the AOA; (3) alternate security procedures for use in emergency and other unusual conditions; and (4) 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.

The indirect air carrier security program covers security procedures for cargo that is accepted for transport on air carrier aircraft. In general, indirect air carriers are required to carry out security procedures for handling cargo that will be carried on air carrier aircraft.

Foreign air carriers' security programs provide security procedures for foreign air carriers while operating to and from the United States, which is a counterpart to the procedures required under part 108.

Security programs of individual companies are based largely on standard security programs and amendments developed by the FAA and industry. As new threats are identified and improved countermeasures developed, the FAA develops standard means to respond to the threats and improve security.

Other sources of information and countermeasures are contained in the Security Directives and Information Circulars, described in § 108.18. These sources address threats to civil aviation security as well as responsive countermeasures to those threats. Additionally, these sources provide sensitive information concerning various security devices, such as metal detectors and X-ray machines.

The Need to Protect Security Information

The notice of proposed rulemaking contained a history of how the threat to civil aviation has increased over the years. The FAA monitors potential threats to civil aviation. Terrorist pose an increasingly sophisticated threat to civil aviation. This has led the FAA to reevaluate the release of security information to the public, particularly in response to requests under the FOIA. This information has been termed sensitive security information (SSI).

It is important to keep details of security measures and FAA evaluations of security out of the public domain where terrorists could read them. If the information identified in this rule were publicly available, it could reveal potential weaknesses in the current security system.

The FAA is mindful of the public's legitimate interest in how the FAA operates and how it regulates the aviation industry, as well as how the industry is carrying out its duties. The FAA has a corresponding responsibility to prevent undue disclosure of information that could compromise public safety if it falls into the wrong hands. The rule has been carefully considered and covers only information

that could reasonably be anticipated to be damaging to the security of the traveling public if given to unauthorized persons.

Security programs are absolutely essential mechanisms through which the FAA regulates the air carriers' and airports' detailed obligations with respect to ensuring civil aviation security. Much of the effectiveness of the programs depends on strictly limiting access to such information to those persons who have a need-to-know. Unauthorized disclosure of the specific provisions of the air carrier and airport security programs or other aviation security information would allow potential attackers of civil aviation to devise methods to circumvent or otherwise defeat the security provisions. It would also discount the deterrent effect inherently provided in prohibiting disclosure of security measures that may or may not be in place.

There are sophisticated criminal elements who actively seek information on what seemingly are minor security points, with a view to accumulating a larger picture of the entire security program. Therefore, it is imperative that the entire security program be protected. Similarly, it is critical to protect the information contained in Security Directives and Information Circulars. These documents contain detailed information on threats that the FAA has identified, and the measures to counter those threats. The unauthorized release of that information could compromise those countermeasures. In addition, particular information regarding FAA approved security devices, such as metal detectors, should also be protected to the extent possible.

Current Protection of Security Information

Currently, the FAA, airport operators, air carriers, indirect air carriers, and foreign air carriers are required to restrict the availability of information contained in security programs to those with a need-to-know, and to refer requests for such information by other persons to the FAA. These requirements are in §§ 107.3(e), 108.7(c) (4) and (5), 109.3(c), and foreign air carrier security programs. In addition, § 108.18(d) specifically requires both air carriers and individuals to restrict the availability of Security Directives and Information Circulars, and the information contained therein, to persons with a need-to-know. However, individuals who work for or perform activities in support of the air carriers are not required to protect other security information.

Part 191 states when the FAA will withhold certain requested information from public disclosure, such as when requested under the Freedom of Information Act (FOIA) (5 U.S.C. 552), in litigation, or in rulemaking. Part 191 currently applies only to the FAA, and does not specify all of the sources of SSI that should be covered.

Civil aviation security information protected under the Federal Aviation Regulations is different from Classified National Security Information governed by Executive Order 12598 and related orders, statutes, and rules. The Executive Order provides for classifying information as Top Secret, Secret, and Confidential, and covers a wide range of information affecting the national security. All persons with access to such information must have an appropriate security clearance, and there may be a criminal penalty for misuse of the information. While there is some ''classified'' civil aviation security information, part 191 is not directed to the handling of classified information. Indeed, part 191 is needed because the SSI is not National Security Information and therefore is not subject to the controls that apply to such information.

This final rule improves the protection of SSI by amending parts 107, 108, 109, 129, and 191 as described more fully later in the document.

Discussion of Comments

The FAA published Notice of Proposed Rulemaking No. 94–32 on December 6, 1994 (59 FR 62956). In response to Notice No. 94–32, 17 comments were received from a total of 18 commenters, 2 commenters having jointly submitted 1 comment.

Five commenters state that the proposed language in proposed § 191.5(a) on the release of SSI is too broad. Of these, two commenters ask the FAA to limit this language by linking the enforcement of SSI unauthorized releases to significant compromises of security or those that result in an actual security incident.

The FAA believes the suggested language would weaken the rule. The FAA should not have to wait to see if the improperly released or compromised information is actually misused before taking action against the person(s) who released it. On the contrary, one purpose of the rule is to have more clear and consistent guidance as to what must be protected. In every case in which the FAA considers what enforcement action to take in response to a violation, however, the FAA considers all factors, including the potential or actual adverse impact on safety or security.

The same two commenters also share the view that the FAA should limit the geographic scope of airport security programs solely to that area where scheduled carriers operate. These commenters argue that this geographic limitation would remove general aviation operations from the Air Operations Area (AOA), reducing the number of individuals with a ''need-to-know'' and thereby reducing the potential for the release of SSI.

The FAA finds that the scope of the airport security program would be more appropriately addressed in Part 107. If needed, airport operators may contact their cognizant FAA security office for a re-evaluation of the geographic areas in which security measures are applied.

Six commenters request the addition of language to proposed § 191.5 (a) or (d) to make clear that, if an air carrier or airport operator has established a reasonable procedure for the control of sensitive information and has not been negligent in monitoring compliance with this procedure, the air carrier or airport operator would not be held to a standard of strict liability for disclosures made by individuals.

Currently § 108.7(c)(4) requires each air carrier to ''restrict the availability of information contained in the security program to those persons with an operational need-to-know * * *'' Current § 107.3(e) requires in part that each airport operator ''restrict the distribution, disclosure, and availability of information contained in the security program to those persons with an operational need-to-know * * *'' Proposed § 191.5(a) would impose similar duties on airport operators and air carriers, stating that they must ''restrict disclosure of and access to sensitive security information to persons with a need-to-know, * * *'' The FAA is not aware that any instance in which an air carrier or airport operator allegedly has been held to an unduly strict standard for compliance with the current rules. Accordingly, no change is needed to the proposal.

Two commenters indicate that, when the FAA releases a Security Directive to the air carriers, the air carriers' principal means of dissemination to the affected locations throughout the world are via facsimile, teletype, and electronic mail messages. The commenters indicate that remote facsimile machines, high speed printers, and computers often are not located in secured areas and operate on a 24-hour schedule due to differences in time zones. The commenters state that, unlike certain government agencies that routinely handle SSI, there are very few air carrier employees, and even fewer contract workers, who hold a

Department of Defense (DOD)-approved SECRET clearance. Nonetheless, the commenters say they do support the premise that individuals should be penalized if they have acted imprudently or knowingly disregarded the instructions of their employers. The commenters state that even with the clearest of instructions regarding the protection of the information, it is unreasonable to expect air carriers to be totally responsible for the actions of a large number of individuals.

As noted earlier in this document, the air carriers' responsibility under the rule will be similar to their responsibilities under the current rule, and air carriers that are in compliance now need not change their procedures.

SSI is not Classified National Security Information, and no Secret clearance issued by the Federal government is required to gain access to it. The FAA realizes that certain employees will have access to SSI simply because they must retrieve the information from facsimile machines and the like, although they do not have responsibility to carry out the security program. All such employees, however, are responsible for protecting the information from unauthorized disclosure.

Three commenters ask how agencies or persons, included within the scope of the proposed regulation, should respond to Freedom of Information Act (FOIA) or Open Records Act (ORA) requests for unclassified security information, in the event the proposed regulation is promulgated as written.

The requirement to make records available under the FOIA does not apply to matters that are specifically exempted from disclosure by statute (5 U.S.C. 552(b)(3)). Under 49 U.S.C. 40119, the information described in the rule is exempt by statute from disclosure. When the FAA receives requests under FOIA for SSI, the FAA will deny the information in accordance with § 191.3. As to requests for information under state and local freedom of information acts or open records acts, § 191.5(a) provides that requests for SSI be referred to the Administrator. The FAA works with the airports and air carriers to determine what records or portions of records should remain undisclosed, and what may be released.

Ten commenters state that the proposed regulation restricts, too severely, the disclosure of SSI. Three of these commenters object that the proposed language may prohibit disclosure of security information to a carrier president, outside counsel, consultant, or management personnel who do not personally perform or directly supervise security activities. Five commenters indicate that the carriers may be required to inform parties other than those with a need-to-know of certain security requirements or procedures. Such parties may include travel agents, passengers, contractors, and internal personnel who develop procedures to ensure effective passenger, cargo, and baggage processing for the air carrier.

The FAA believes that the definition of ''need-to-know'' as proposed would have provided for dissemination of information to travel agents, passengers, contractors, and internal personnel, when such dissemination is necessary to carry out security duties. The FAA agrees, however, that the proposed definition could have been read as more limiting than intended, as to some persons. Various high level officials must be apprised of the information, even though they may not personally carry out the security requirements. Further, persons who represent the air carriers and airport operators, such as attorneys and industry associations, may have a need-to-know, in order to be able to represent their clients. In order to avoid misunderstanding, the FAA is clarifying the definition of need-to-know in § 191.5(b) to read as follows: A person has a need-to-know sensitive security information when the information is necessary to carry out FAA-approved or directed aviation security duties; when the information is necessary to supervise or otherwise manage the individuals carrying out such duties; to advise the airport operator, air carrier, indirect air carrier, or foreign air carrier regarding the specific requirements of any FAA security related requirements; or to represent the airport operator, air carrier, indirect air carrier, or foreign air carrier, or person receiving information under § 191.3(d) in connection with any judicial or administrative proceeding regarding those requirements. For some specific information, the Administrator may specify which persons, or classes of persons, have a need-to-know.

Three commenters indicate that contractors who are bidding on a job inside the security identification display area (SIDA) need to know that the procedures are for ID applications and employment history checks in order to price their bids correctly. One of these commenters states that ''each person issued an airport identification badge has a need to know certain details of the Airport Security Program.''

The definition of ''need-to-know'' in § 191.5(b) includes the need for the information to carry out FAA approved or directed aviation security duties. When a contractor needs the procedures for ID applications and employment checks in order to comply with FAA rules and the airport security program, the contractor has a ''need-to-know'' within the meaning of the rule. Such releases of information must be limited only to the information needed to comply.

One commenter states that, in most international locations, air carriers do not provide their own security. According to this commenter, the security at international locations comes in the form of assistance provided by the host government. This commenter states that, in order to carry out some of the FAA-mandated security directives, some portion of those directives must be disclosed to the host government. In this commenter's opinion, the proposed draft acknowledges that the foreign government has a need-to-know in the case of a foreign air carrier, but not necessarily in connection with the overseas operation of a U.S. air carrier.

The FAA finds that the foreign government would also meet the need-to-know requirement in connection with the overseas operations of a U.S. air carrier. Procedures have already been established through FAA liaison personnel and the State Department to communicate necessary security information.

Two commenters state that many airport operators must supply monthly confiscated weapons reports or incident reports to other official bodies, sometimes for the purpose of prosecution at the local level. Another commenter notes that, local law enforcement or legislative requirements may require disclosure of certain security information to persons otherwise without a ''need-to-know'' as part of normal reporting requirements. This commenter requests coordination among industry and FAA personnel before the FAA designates information as ''sensitive.''

It appears that most confiscated weapons reports would not be SSI, if the airport operator is releasing the report. Section 191.7(h) makes such information SSI only as to release by the FAA. As to the release of other information to law enforcement officials, or in response to other legislative requirements, the airport operator should contact the FAA to discuss specific needs. Some of the information the commenter is concerned about may not be SSI under the rule. As to information that is SSI, the FAA may approve release to specific states and local officials with appropriate safeguards to prevent its dissemination to unauthorized persons.

One commenter indicates that, if sensitive information concerns a specific airport, persons having a need-to-know should include, at a minimum, the designated Airport Security Coordinator(s). This commenter also states that Coordinators should have the authority to disseminate such information themselves on a need-to-know basis among parties at the airport or within the same airport authority.

The FAA agrees with the commenter to the extent that the need-to-know requirements apply.

One commenter states that the proposed disclosure limitations may preclude carriers from seeking assistance form government agencies or other law enforcement authorities when faced with unusual security situations or threats.

It appears that, if the air carrier is seeking assistance to respond to security situations or threats, there is a need-to-know within the meaning of the rule. Of course, the agency or authority should be informed of the nature of the information and the need to not release it to unauthorized persons.

One commenter asks that proposed § 191.5(c) be modified to include whistle-blower protection for the entity that advises the FAA that a breach of security has occurred. This commenter observes that, ''without a safeguard, there will be a tendency for parties * * * not to advise the FAA (that a breach of security has occurred) in the hope that they would not be caught * * *.''

The primary purpose of § 191.5(c) is to permit the FAA to evaluate the release of information and determine whether there is a need to act to mitigate any vulnerability the release might have caused. The fact that a person self-discloses a failure to comply with the rule is given significant weight in determining what, if any, action should be taken as to that person. In the end, the choice of action involves the exercise of prosecutorial discretion, and will be considered in the context of policies involving enforcement in general.

Four commenters ask for modification of proposed § 191.5(d) to specify the FAA's criteria for adequate restriction of access to, or disclosure of, sensitive information; to clarify what changes might be recommended by the FAA to security procedures; and to state the actions that may be included in the phrase ''other enforcement or corrective action,'' including potential criminal prosecution.

As noted previously, the air carriers' and airport operators' responsibilities under the new rule are similar to their responsibilities under the current rules. Procedures that are appropriate under the current rules should be continued. and a similar level of protection should be used for other SSI.

It is not possible to list changes to security procedures that might be required after an unauthorized release of those procedures. It would depend on what information was released, the apparent security risk resulting from the release, and what other measures might be considered appropriate alternatives to those that were compromised. In addition, the FAA might consider requiring changes to the way SSI was handled or disseminated, if it was discovered that the air carrier or airport operator had inadequate procedures.

The types of possible action the FAA might take in response to a violation are set forth in the statute and FAA Order 2150.3A, compliance and Enforcement Program. These include such actions as counseling, corrective action, civil penalties. and certificate action (such as suspension or revocation of a certificate). In appropriate cases, the FAA may refer a matter to proper authorities for criminal prosecution.

Two commenters request modification of proposed § 191.7 to list, as completely as possible, the specific categories of information which fall within the meaning of the phrase SSI. These commenters state that such a list should include training programs and records of practice exercise as a category.

The entire training program of an air carrier is not normally SSI. However, the program contains SSI, such as specifications of test objects and security devices, and sensitive procedures. Under § 191.7, the portions of the training programs containing SSI must be protected, but the rest is not subject to this rule.

Similarly, training records are not normally considered SSI in themselves, because they normally do not contain SSI. They may simply indicate the dates that the screeners completed their training, for instance. Such records are a general means by which the FAA monitors industry compliance with specific requirements, and therefore would not require protection in accordance with § 191.7. However, there are occasions when information related to ''sensitive activities,'' such as practical exercise, which falls under the purview of)191.7(d), is included in training records. Under these circumstances, these particular training records would be subject to part 191 controls.

These two commenters also ask whether the airport boundary descriptions found in airport security plans are SSI, whether information that is readily available elsewhere become SSI by being included in an airport security plan, whether partial disclosures of information contained in an airport security plan might violate the proposed regulation, and if so, what the threshold of violation by partial disclosure might be.

Informaiton that is not in the security plan or otherwise listed in § 191.7 is not SSI under this rule. Because the airport boundary descriptions are readily available elsewhere, they can be released in the form that is available elsewhere without violating the new rule.

These commenters also suggest that the FAA reconsider the necessity of designating all threat information as sensitive. According to these commenters, it would be more efficient to draw a distinction between information regarding general trends in terrorist technology and possible responses, which is largely in the public domain and should not be subjected to extensive disclosure protection, and known, specific threats.

It is not clear to which portion of the rule the commenters are objecting. New § 191.7(i) (proposed as § 191.7(h)(1)) makes threat information SSI only as to release by the FAA, which means that the FAA may decline to release the information. That section does not require the airport operator or air carrier to protect the information. Airport operators and air carriers are required to protect threat information that may be a part of security program amendments, Security Directives, and Information Circulars, because they are protected under § 191.7 (a) and (b). It should also be noted that general trends in terrorist technology and possible responses often is non-public, and may even be Classified National Security Information.

Two commenters state that the FAA cost/benefit analysis is not correct. Of these, one commenter states that evidence does not exist to support the FAA's portrayal of the terrorist threat to civil aviation, as found in the section of the NPRM titled ''The Need To Protect Security Information.''

The FAA disagrees with this commenter. The information reflected in the ''Need To Protect Security Information'' section of the NPRM is based on a complete analysis of the best threat information available.

The other commenter in this group states that, if the proposed regulation is adopted, the air carriers will have to inform their employees of the new regulations and will also have to design

a more sophisticated tracking system in order to trace the dissemination of security information. Dollars will have to be spent to secure information in safes, locked rooms, and to purchase shredders and conduct audits. The commenters state that there is the potential cost to the carriers to investigate and respond to FAA allegations of noncompliance, which more often than not results in a civil penalty.

Again, the air carriers' and airport operators' responsibilities under the new rules are similar to their responsibilities under the current rules. Procedures that are appropriate under the current rules should be continued, and a similar level of protection should be used for all designated SSI.

One commenter indicates that the FAA has underestimated the proposed regulation's constitutional implications for restriction of freedom of speech.

The commenter does not provide an analysis as to how the Constitution protections of freedom of speech are violated. The FAA considers that restricting dissemination of the information described in the rule is necessary to protect the traveling public from persons who would seek to commit acts of criminal violence or aircraft piracy. The FAA has attempted to include as little information as is reasonably necessary to adequately protect the public.

The Rule As Adopted

Part 191

Part 191 sets forth the rules that allow the FAA to withhold information from public disclosure. This final rule amends and reorganizes part 191 as follows:

Section 191.1 is expanded to apply not only to the FAA, but also to air carriers, airport operators, indirect air carriers, foreign air carriers, and individuals. As discussed later in this document, parts 107, 108, 109, and 129 still would contain some requirements regarding the protection of information, but part 191 would be the primary rule for withholding information from unauthorized disclosure.

Section 191.1(a) is amended to conform to the current statute. In 1976, the FAA promulgated part 191 to implement the Air Transportation Act of 1974, Public Law 93–366. Section 316(d)(2) of the Federal Aviation Act of 1958, as amended, provided, in part, that the Administrator shall prescribe regulations to ''prohibit disclosure of any information obtained or developed in the conduct of research and development activities'' if the disclosure meets certain conditions. This section is a major basis for the current rules in part 191 on withholding information from unauthorized disclosure.

In 1990, section 316(d)(2) was amended to provide that the Administrator shall adopt rules to prohibit disclosure of ''any information obtained in the conduct of security *or* research and development activities. * * *'' Section 9121 of the Aviation Safety and Capacity Expansion Act of 1990 (Pub. L. 101–508) (emphasis added). In 1994 this section was recodified, and now appears at 49 U.S.C. 40119. This final rule amends § 191.1(a), to protect information obtained during the course of specified security activities. This final rule also removes from the title of part 191 reference to the 1974 Act, to avoid any implication that it is the only source of statutory authority for the part.

Section 191.1(b) now defines ''record,'' in part, as ''documentary'' material. This final rule removes the word ''documentary.'' It addresses all methods of preserving information, including computer records. This would avoid any misunderstanding over whether such records were ''documentary.''

Part 191 now refers to the ''Director of Civil Aviation Security'' as the official who makes the determination on behalf of the Administrator to withhold information. Under internal FAA reorganization, the current title of this position is Associate Administrator for Civil Aviation Security, however, 49 U.S.C. 44932 refers to this official as Assistant Administrator for Civil Aviation Security. Therefore, part 191, as adopted, used the title ''Assistant Administrator for Civil Aviation Security.'' In addition, the Deputy Assistant Administrator for Civil Aviation Security (currently called the Deputy Associate Administrator for Civil Aviation Security) and any individual formally designated to act in the capacity of the Assistant Administrator or the Deputy, now has the authority to make such determinations.

For decisions involving information and records described in § 191.7 (a) through (g), and related documents in (l), § 191.1(c) permits delegation below the Assistant Administrator level. The information that is described in § 191.7 (a) through (g) is well-defined, and decisions on release or withholding of the information involves relatively objective judgments.

Section 191.7 (h), (i), (j), (k), and related documents described in (l), require more subjective judgments. A decision to release or withhold information under these paragraphs requires a careful evaluation of the need to provide the highest level of security to the traveling public by preventing SSI from falling into the wrong hands, balanced by an awareness of the public's strong interest in obtaining information about security in air transportation. These decisions require a careful evaluation of security threats as well as important policies of the agency. Therefore, this rule requires that such decisions be made by high policy-level officials, and not below the Assistant Administrator and Deputy Assistant Administrator level. The Assistant Administrator is responsible for carrying out the agency's civil aviation security program, and reports directly to the Administrator.

Section 191.3 continues to state generally that the FAA withholds certain information, but has been clarified to state that part 191 applies, notwithstanding FOIA and other disclosure statutes. For example, the FAA may adopt certain security rules affecting air carriers and airports without disclosing the rules to unauthorized persons. Additionally, this rule will move the provisions that describe the circumstances under which the FAA prohibits disclosure of information from § 191.5 to § 191.3(b).

New § 191.3(d) is added to clarify how SSI is handled during enforcement actions. When the FAA initiates legal enforcement action in a matter involving security, if the alleged violator or his designated representative so requests, the Chief Counsel, or designee, may provide copies of portions of the enforcement investigative report (EIR), including SSI. This information may be released only to the alleged violator or designated representative for the sole purpose of providing the information necessary to prepare a response to the allegations contained in the legal enforcement action document. Such information is not released under the FOIA.

Whenever such documents are provided to an alleged violator or designated representative, the Chief Counsel or designee advises the alleged violator or designated representative that: (a) The documents are provided for the sole purpose of providing the information necessary to respond to the allegations contained in the legal enforcement action document; and (b) SSI contained in the documents provided must be maintained in a confidential manner to prevent compromising civil aviation security.

Section 191.5, as adopted, contains the requirements that apply to persons other than the FAA. Such persons

include air carriers, airport operators, indirect air carriers, foreign air carriers, and persons who receive SSI in connection with enforcement actions, and individuals employed by, or contracted by, air carriers, airport operators, indirect air carriers, foreign air carriers, and persons who receive SSI in enforcement actions. This section is intended to be very inclusive.

A difficult aspect of protecting SSI is that a large number of persons must be aware of at least portions of the information in order to carry out their duties including pilots, flight attendants, ticket agents, screeners, baggage handlers, and law enforcement officers. Frequently, some of these people are not direct employees of the air carrier or airport operator, but they do carry out duties for, or on behalf of, the air carrier or airport operator. For example, in many cases, screeners and law enforcement officers are not directly employed by air carriers or airport operators, but do have important security responsibilities to carry out. This section is intended to cover all such persons who have access to SSI. It should be emphasized, however, that airports and air carriers will continue to have the responsibility they now have to protect SSI. If SSI is released to unauthorized persons, depending upon the circumstances, the FAA may hold the airport or air carrier, as well as the individual accountable.

Section 191.5(a) states the general requirement that disclosure of, and access to, SSI shall be restricted to persons with a need-to-know. Section 191.5(b) defines need-to-know as when the information is necessary to carry out FAA-approved or directed aviation security duties; when the information is necessary to supervise or otherwise manage the individuals directly carrying out such duties; to advise the airport operator, air carrier, indirect air carrier, or foreign air carrier regarding the specific requirements of any FAA security related requirements; or to represent the airport operator, air carrier, indirect air carrier, or foreign air carrier, or person receiving information under § 191.3(d) in connection with any judicial or administrative proceeding regarding those requirements.

In most cases, the air carrier or airport operator has the discretion to decide who in its organization has a need to know SSI. There are times, however, when information is so sensitive that extra measures should be taken to protect that information from release to those without a need-to-know. The rule would, therefore, provide that for some specific information the Administrator may make a finding that only specific persons, or classes of persons, have a need-to-know.

Section 191.5(c) requires that, if sensitive security information is released to unauthorized persons, the FAA must be notified. This will permit the FAA to evaluate the risk presented by the release of the information, and to take whatever action may be needed to mitigate that risk.

Section 191.5(d) alerts persons that violations may result in a civil penalty or other action by the FAA. The FAA may take a broad range of enforcement action for violation of the regulations. The FAA anticipates that civil penalty action will be considered for a violation of part 191, as it is for violations of parts 107 and 108. However, the FAA may seek enforcement action deemed appropriate based on individual circumstances of the case. Further, the FAA may take action to mitigate or correct the risk posed by the violation. Such actions may include requiring air carriers or airport operators to change their procedures for protecting security information, or change the security procedures in place that may have been compromised by unauthorized release of the information.

New § 191.7 describes information that is protected from public disclosure. Some of this information is now specifically described in current § 191.3, and the rest the FAA now withholds based on findings under current § 191.5, in that disclosure of this information would be detrimental to the safety of persons traveling in air transportation or intrastate air transportation. These findings are set forth in written denials of FOIA requests for such information, and in declarations submitted to judges to seek protection of information in litigation cases. To better inform the public of the information prohibited from unauthorized release, this rule adds this information to new § 191.7.

The introductory text of § 191.7 provides that the specified information is SSI, ''except as otherwise provided in writing by the Administrator.'' This exception serves two functions. First, some SSI contains information that is released to the public, and the FAA may issue press releases and otherwise make this information available. Air carriers and others would not be expected to protect those details.

Second, the Administrator may release some other SSI to help achieve compliance with the security requirements. In rare circumstances the FAA has released summary information regarding air carriers' failures to fully carry out their security duties, which assisted in bringing them into compliance. In such cases, the FAA must determine whether security will be better served by maintaining the confidentiality of the information, or to release some portions of it to help achieve compliance with the security standards.

The introductory text of § 191.7 also refers to ''records containing such information'' as being SSI. This would include, for instance, interpretations that contain information on the contents of security programs and other SSI.

Section 191.7(a) retains the current requirements to protect any approved or standard security program for an air carrier, indirect air carrier, airport operator, or foreign air carrier. It also is clarified to protect any security program that relates to United States mail to be transported by air (including that of the United States Postal Service and of the Department of Defense). This rule expands this provision to include any comments, instructions, or implementing guidance pertaining to these security programs. Generally, these materials reveal some or all of the sensitive information and must be protected the same as the security programs themselves.

Section 191.7(b) is revised to include any comments, instructions, or implementing guidance pertaining to Security Directives and Information Circulars.

New § 191.7(c) lists any profile used in any security screening process, including persons, baggage, or cargo. Hijacker and baggage screening profiles were previously addressed in current § 191.3(b) (1) and (2). This rule now makes those profiles general to cover screening persons, because there are systems in place to protect against terrorists and others who might seek to commit criminal violence, not just hijackers. This rule addresses cargo profiles because, like baggage, cargo is a potential tool for criminal violence that the security rules cover.

Section 191.7(d) includes any security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto. These plans, when adopted, become part of the security program and are already covered by rules governing security programs; however, they are included in § 191.7 for emphasis.

This rule deletes the provisions currently in current § 191.3(b)(6), pertaining to the technical specifications for devices for protection against, or detection of, cargo theft. Such devices are not directly used to meet the requirements for civil aviation security under the FAA regulations. Any devices that serve a dual function of protecting cargo and security are

protected under other provisions in this section.

Section 191.7(e) covers the technical specifications of any device used for the detection of any ''deadly or dangerous weapon, explosive, incendiary, or destructive substance.'' It is essentially the same as the current § 191.3(b)(5) which used the words ''explosive or incendiary device or weapon,'' with the addition of the phrase ''destructive substance.'' That phrase is used in 49 U.S.C. 44902 in reference to searching persons and property to be carried aboard aircraft.

Section 191.7(f) addresses the descriptions of and technical specifications of objects used to test screening equipment and equipment parameters. Knowledge of this test equipment and parameters could lead to a plan to defeat those devices. Accordingly, details of such devices should be protected.

Section 191.7(g) addresses the technical specifications of any security communications equipment and procedures. Knowledge of security communication equipment and procedures could lead to a plan to defeat those devices. Accordingly, details of such devices should be protected.

Section 191.7(h) addresses release of certain information relating to violation of the security rules. Section 191.7(h) applies only to the release of information by the FAA. There is less risk of harm from casual disclosure of this information by individuals. The FAA, however, has information regarding the entire security system. Release of significant amounts of such information by the FAA could permit someone to attempt to identify weaknesses in the system that might be exploited.

The notice proposed in § 191.7(h)(2) to withhold the details of alleged violations of parts 107, 108, 109, or 129, including the airport name, the location of the gate or access point; the air carrier, indirect air carrier, or foreign air carrier, and any information that could reasonably lead to the disclosure of such details. After further consideration, the FAA has determined that this proposed policy was more restrictive than necessary. The rule as adopted makes a distinction between information based on the time since the incident occurred. In the first 12 months, there is the highest level of concern that information could be used to identify an apparent weakness that an unauthorized person may seek to exploit. After 12 months, there has been sufficient passage of time, including an opportunity to correct any deficiency in the system, to make that information less useful in identifying apparent weaknesses.

Section 191.7(h) as adopted provides generally for withholding any information that the Administrator has determined may reveal a systemic vulnerability of the aviation system or a vulnerability of aviation facilities to attack. This is defined to include certain details of inspections, investigations, and alleged violations and findings of violations of 14 CFR parts 107, 108, or 109, or §§ 129.25, 129.26, or 129.27, and any information that could lead to the disclosure of such details. For events that occurred less than 12 months before the date of the release of the information, the FAA will not release the name of an airport where a violation occurred, the regional identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of the air carrier in connection with specific locations or specific security procedures. The FAA may release summaries of an air carrier's total security violations in a specified time range without identifying specific violations. Summaries may include total enforcement actions, total proposed civil penalty amounts, total assessed civil penalty amounts, number of cases opened, number of cases referred by Civil Aviation Security to FAA counsel for legal enforcement action, and number of cases closed.

For events that occurred 12 months or more before the date of the release of the information, FAA will not release the specific gate or other location on an airport where the event occurred.

In addition, the FAA will not release the identity of the FAA special agent who conducted the investigation or inspection, or security information or data developed during FAA evaluations of the air carriers and airports and the implementation of the security programs, including air carrier and airport inspections and screening points tests or methods for evaluating such tests.

Section 191.7(i) (proposed as § 191.7(h)(1)) covers release by the FAA of information concerning threats against civil aviation. This paragraph specifically applies only to release of information by the FAA. However, threat information may also be contained in Security Directives, Information Circulars, or other documents that air carriers and others must protect under other provision of this section.

Section 191.7(j) further clarifies that the FAA does not release, and others should not release, certain details of security measures not otherwise listed in this section, such as information regarding Federal Air Marshals. Release of such information to unauthorized persons could not only compromise security, it could place Federal Air Marshals in danger.

Secton 191.7(k) includes any other information that the Administrator determines should not be disclosed under the criteria in § 191.3(b). While we have attempted to anticipate all sources of information that should be protected from unauthorized disclosure, additional information may be discovered in the future. This section allows the Administrator to determine whether that additional information should or should not be considered as SSI.

Section 191.7(1) includes any draft, proposed, or recommended changes to SSI or records. The FAA frequently issues proposed revisions for sensitive security documents to air carriers and airports operators and requests comments on the proposals. These proposals contain SSI that also should be protected.

Parts 107, 108, 109 and 129

This rule change also affects those specific sections of parts 107, 108, 109, and 129 which require airport operators, air carriers, indirect air carriers, and foreign air carriers to protect security information and direct requests for such information to the administrator as required in part 191.

All changes to parts 107, 108, 109, and 129 correspond to, and are redundant with, changes made to part 191 because airport operators, air carriers, and foreign air carriers refer to their specific parts of Title 14 CFR for security requirements. Including a cross-reference to part 191 in parts 107, 108, 109, and 129, alerts airport operators and air carriers to the new requirements, and makes it clear that part 191 is part of their security duties.

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), there are not requirements for information collection associated with this final rule.

International Compatibility

The FAA has reviewed corresponding International Civil Aviation Organization international standards and recommended practices and Joint Aviation Airworthiness Authorities requirements and has identified no differences in these amendments and the foreign regulations.

Regulatory Evaluation Summary

Benefits and Costs

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866 directs that each Federal agency shall 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 requires agencies to analyze the economic effect of regulatory changes on small entities. Third, the Office of Management and Budget directs agencies to assess the effect of regulatory changes on international trade. In conducting these analyses, the FAA has determined that this rule is not ''a significant regulatory action'' as defined in the Executive Order and the Department of Transportation Regulatory Policies and Procedures. This rule will not have a significant impact on a substantial number of small entities and will not constitute a barrier to international trade.

A detailed discussion of costs and benefits is contained in the full evaluation in the docket for this Final rule. The costs and benefits associated with this Final rule are summarized as follows.

Air carriers and airports have security programs which are intended to protect the public from the threat of aircraft hijacking and other criminal activities affecting air transportation. The FAA proposes to strengthen the rules protecting security-related information from being released to unauthorized persons. The current rules fail to require individuals to protect sensitive security information that is in their control, and specify all sensitive security information that should be protected from public disclosure.

The unauthorized disclosure of any of the information contained in these security programs can have a detrimental effect on the ability to thwart terrorist and other criminal activities. This final rule will amend parts 107, 108, 109, and 129 to restrict the distribution, disclosure, and availability of specific sensitive security information, which will be defined in part 191, to persons with a need-to-know.

Because this fine rule will not be included in the airport or the air carrier security programs, and because there are no specific requirements for safes, locked files, or enhanced security equipment, affected entities will not incur any costs to implement these proposed requirements.

Much of the air carrier and airport security program effectiveness depends on strictly limiting access to sensitive security information to those persons who have a need to know. Sophisticated criminal elements are actively seeking ways to obtain information regarding the methods and procedures used by the FAA, air carriers, and airports to guard against terrorist activities. The accumulation of seemingly minor security details can enable the criminal element to piece together a larger picture of the entire security program. Therefore, it is imperative that the entire security program be protected.

The consequences of not protecting such information can be catastrophic. Between 1982 and 1991, terrorist bombings of U.S. air carriers have resulted in 275 deaths and 24 injuries, while hijackings incidents have resulted in 24 deaths and 127 injuries.

Given the absence of cost and the potential benefits of avoided fatalities and injuries, this final rule is cost beneficial.

Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980 (RFA) was enacted by Congress to ensure that small entities are not unnecessarily burdened by government regulations. The RFA requires agencies to review rules that may have a ''significant economic impact on a substantial number of small entities.'' FAA Order 2100.14A, Regulatory Flexibility Criteria and Guidance, establishes threshold costs and small entity size standards for complying with RFA requirements. There is no cost associated with this rule; therefore, it does not have a significant economic impact on a substantial number of small entities.

International Trade Impact Statement

In accordance with the Office of Management and Budget memorandum dated March 1983, federal agencies engaged in rulemaking activities are required to assess the effects of regulatory changes on international trade. The FAA finds that this rule will not have an adverse impact on trade opportunities for either U.S. firms doing business overseas or foreign firms doing business in the United States. This rule will impose no costs on both domestic and foreign air carriers, so neither would have a trade advantage over the other.

Federalism Implications

This rule 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, in accordance with Executive Order 12612, it is determined that this rule does not have sufficient federalism implications to warrant preparation of a Federalism Assessment.

Conclusion

For the reasons discussed above, and based on the findings in the Regulatory Flexibility Determination and the International Trade Impact Statement, the FAA certifies that this regulation will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act. This rule is not considered a ''significant regulatory action'' under Executive Order 12866 and is considered nonsignificant under Order DOT 2100.5, Policies and Procedures for Simplification, Analysis, and Review of Regulations. A regulatory evaluation of the rule, including a Regulatory Flexibility Determination and international Trade Impact Analysis, has been placed in the docket. A copy may be obtained by contracting the person identified under **FOR FURTHER INFORMATION CONTACT.**

List of Subjects

14 CFR Part 107

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

14 CFR Part 108

Air carriers, Aircraft, Airmen, Airports, Arms and munitions, Explosives, Law enforcement officers, Reporting and recordkeeping requirements, Security measures, X-rays.

14 CFR Part 109

Air carriers, Aircraft, Freight forwarders, Security measures.

14 CFR Part 129

Air carriers, Aircraft, Aviation safety, Reporting and recordkeeping requirements, Security measures, Smoking.

14 CFR Part 191

Air transportation, Security measures.

The Amendment

Accordingly, the Federal Aviation Administration amends parts 107, 108, 109, 129, and 191 of Title 14, Code of Federal Regulations (14 CFR parts 107, 108, 109, 129, and 191) as follows:

PART 107—AIRPORT SECURITY

1. The authority citation for part 107 continues to read as follows:

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

2. Section 107.3 is amended by revising paragraph (e) to read as follows:

§ 107.3 Security program.

* * * * *

(e) Each airport operator shall—

(1) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 191 of this chapter, to persons with a need-to-know; and

(2) Refer requests for security sensitive information by other persons to the Assistant Administrator for Civil Aviation Security.

PART 108—AIRPLANE OPERATOR SECURITY

3. The authority citation for part 108 continues to read as follows:

Authority: 49 U.S.C. 106(g), 5103, 40113, 40119, 44701–44702, 44705, 44901–44905, 44907, 44913–44914, 44932, 44935–44936, 46105.

4. Section 108.7 is amended by revising paragraphs (c)(4) and (c)(5) to read as follows:

§ 108.7 Security program: Form, content, and availability.

* * * * *

(c) * * *

(4) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 191 of this chapter, to persons with a need-to-know; and

(5) Refer requests for sensitive security information by other persons to the Assistant Administrator for Civil Aviation Security.

PART 109—INDIRECT AIR CARRIER SECURITY

5. The authority citation for part 109 continues to read as follows:

Authority: 49 U.S.C. 106(g), 5103, 40113, 40119, 44701–44702, 44705, 44901–44905, 44907, 44913–44914, 44932, 44935–44936, 46105.

6. Section 109.3 is amended by revising paragraph (c) to read as follows:

§ 109.3 Security program.

* * * * *

(c) Each indirect air carrier shall—

(1) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 191 of this chapter, to persons with a need-to-know; and

(2) Refer requests for sensitive security information by other persons to the Assistant Administrator for Civil Aviation Security.

PART 129—OPERATIONS: FOREIGN AIR CARRIERS AND FOREIGN OPERATORS OF U.S.-REGISTERED AIRCRAFT ENGAGED IN COMMON CARRIAGE

7. The authority citation for part 129 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40104–40105, 40113, 40119, 44701–44702, 44712, 44716–44717, 44722, 44901–44904, and 44906.

8. Part 129 is amended by adding a new § 129.31 to read as follows:

§ 129.31 Airplane security.

Each foreign air carrier required to adopt and use a security program under § 129.25(b) shall—

(a) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 191 of this chapter, to persons with a need-to-know; and

(b) Refer requests for sensitive security information by other persons to the Assistant Administrator for Civil Aviation Security.

9. Part 191 is revised to read as follows:

PART 191—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.

Authority: 49 U.S.C. 106(g), 5103, 40113, 40119, 44701–44702, 44705–44706, 44901–44907, 44913–44914, 44932, 44935–44936, 46105.

§ 191.1 Applicability and definitions.

(a) This part governs the release, by the Federal Aviation Administration and by other persons, of records and information that has been obtained or developed during security activities or research and development activities.

(b) For purposes of this part, *record* includes any writing, drawing, map, tape, film, photograph, or other means by which information is preserved.

(c) 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 other individual formally designated to act in their capacity. For matters involving the release or withholding of information and records containing information described in § 191.7 (a) through (g), and related documents described in (l), the authority may be further delegated. For matters involving the release or withholding of information and records containing information described in § 191.7 (h) through (k), and related documents described in (l), the authority may not be further delegated.

§ 191.3 Records and information withheld by the Federal Aviation Administration.

(a) Except as provided in § 191.3 (c) and (d), and notwithstanding 5 U.S.C. 552 or other laws, the records and information described in §§ 191.7 and 191.3(b) are not available for public inspection or copying, nor is information contained in those records released to the public.

(b) The Administrator prohibits disclosure of information developed in the conduct of security or research and development activities under 49 U.S.C. 40119 if, in the opinion of the Administrator, the disclosure of such information would:

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the safety of persons traveling in air transportation.

(c) If a record contains information that the Administrator determines cannot be disclosed under this part, but also contains information that can be disclosed, the latter information, on proper Freedom of Information Act request, will be provided for public inspection and copying.

However, if it is impractical to redact the requested information from the document, the entire document will be withheld from public disclosure.

(d) After initiation of legal enforcement action, if the alleged violator or designated representative so requests, the Chief Counsel, or designee, may provide copies of portions of the enforcement investigative report (EIR), including sensitive security information. This information may be released only to the alleged violator or designated representative for the sole purpose of providing the information necessary to prepare a response to the allegations contained in the legal enforcement action document. Such information is not released under the Freedom of Information Act. Whenever such documents are provided to an alleged violator or designated representative, the Chief Counsel or designee advises the alleged violator or designed representative that—

(1) The documents are provided for the sole purpose of providing the information necessary to respond to the allegations contained in the legal enforcement action document; and

(2) Sensitive security information contained in the documents provided must be maintained in a confidential manner to prevent compromising civil aviation security, as provided in § 191.5 of this part.

§ 191.5 Records and information protected by others.

(a) Each airport operator, air carrier, indirect air carrier, foreign air carrier, and person receiving information under § 191.3(d) of this part; and each individual employed by, contracted to, or acting for an airport operator, air carrier, indirect air carrier, or foreign air carrier; and each person receiving information under § 191.3(d) of this part, shall restrict disclosure of and access to sensitive security information described in § 191.7 (a) through (g), (j), (k), and as applicable (l), to persons with a need-to-know, and shall refer requests by other persons for such information to the Administrator.

(b) A person has a need-to-know sensitive security information when the information is necessary to carry out FAA-approved or directed aviation security duties; when the information is necessary to supervise or otherwise manage the individuals carrying out such duties; to advise the airport operator, air carrier, indirect air carrier, or foreign air carrier regarding the specific requirements of any FAA security related requirements; or to represent the airport operator, air carrier, indirect air carrier, foreign air carrier, or person receiving information under § 191.3(d) of this part, in connection with any judicial or administrative proceeding regarding those requirements. For some specific information the Administrator may make a finding that only specific persons, or classes of persons, have a need-to-know.

(c) When sensitive security information is released to unauthorized persons, any air carrier, airport operator, indirect air carrier, foreign air carrier, or individual with knowledge of the release shall inform the Administrator.

(d) Violation of this section is grounds for a civil penalty and other enforcement or corrective action by the FAA.

§ 191.7 Sensitive security information.

Except as otherwise provided in writing by the Administrator as necessary in the interest of safety of persons traveling in air transportation, the following information and records containing such information constitute sensitive security information:

(a) Any approved or standard security program for an air carrier, foreign air carrier, indirect air carrier, or airport operator, and any security program that relates to United States mail to be transported by air (including that of the United States Postal Service and of the Department of Defense); and any comments, instructions, or implementing guidance pertaining thereto.

(b) Security Directives, Information Circulars, and any comments, instructions, or implementing guidance pertaining thereto.

(c) Any profile used in any security screening process, including for persons, baggage, or cargo.

(d) Any security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto.

(e) Technical specifications of any device used for the detection of any deadly or dangerous weapon, explosive, incendiary, or destructive substance.

(f) A description of, or technical specifications of, objects used to test screening equipment and equipment parameters.

(g) Technical specifications of any security communications equipment and procedures.

(h) As to release of information by the Administrator: Any information that the Administrator has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities, to attack. This includes, but is not limited to, details of inspections, investigations, and alleged violations and findings of violations parts 107, 108, or 109, or § 129.25, 129.26, of § 129.27 of this chapter, and any information that could lead the disclosure of such details, as follows:

(1) As to events that occurred less than 12 months before the date of the release of the information, the following are not released: the name of an airport where a violation occurred, the regional identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of the air carrier in connection with specific locations or specific security procedures. The FAA may release summaries of an air carrier's total security violations in a specified time range without identifying specific violations. Summaries may include total enforcement actions, total proposed civil penalty amounts, total assessed civil penalty amounts, number of cases opened, number of cases referred by Civil Aviation Security to FAA counsel for legal enforcement action, and number of cases closed.

(2) As to events that occurred 12 months or more before the date of the release of information, the specific gate or other location on an airport where an event occurred is not released.

(3) The identity of the FAA special agent who conducted the investigation or inspection.

(4) Security information or data developed during FAA evaluations of the air carriers and airports and the implementation of the security programs, including air carrier and airport inspections and screening point tests or methods for evaluating such tests.

(i) As to release of information by the FAA: Information concerning threats against civil aviation.

(j) Specific details of aviation security measures whether applied directly by the FAA or regulated parties. This includes, but is not limited to, information concerning specific numbers of Federal Air Marshals, deployments or missions, and the methods involved in such operations.

(k) Any other information, the disclosure of which the Administrator has prohibited under the criteria of 49 U.S.C. 40119.

(l) Any draft, proposed, or recommended change to the information and records identified in this paragraph.

Issued in Washington, DC on March 13, 1997.

Barry Valentine,

Acting Administrator.

[FR Doc. 97–6948 Filed 3–20–97; 8:45 am]

BILLING CODE 4910–13–M