



# Federal Register

---

**Tuesday,  
July 19, 2005**

---

**Part V**

## **Department of Homeland Security**

---

**Transportation Security Administration**

---

**49 CFR Parts 1520, 1540, and 1562  
Ronald Reagan Washington National  
Airport: Enhanced Security Procedures  
for Certain Operations; Interim Final  
Rule**

**DEPARTMENT OF HOMELAND  
SECURITY**

**Transportation Security Administration**

**49 CFR Parts 1520, 1540, and 1562**

[Docket No. TSA-2005-21866; Amendment Nos. 1520-3, 1540-6, 1562-1]

RIN 1652-AA49

**Ronald Reagan Washington National  
Airport: Enhanced Security  
Procedures for Certain Operations**

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

**ACTION:** Interim final rule; request for comments.

**SUMMARY:** Since September 11, 2001, general aviation aircraft operations have been prohibited at Ronald Reagan Washington National Airport (DCA). The Transportation Security Administration (TSA) is issuing this interim final rule (IFR) to restore access to DCA for certain aircraft operations while maintaining the security of critical Federal Government and other assets in the Washington, DC metropolitan area. This IFR applies to all passenger aircraft operations into or out of DCA, except U.S. air carrier operations operating under a full security program required by 49 CFR part 1544 and foreign air carrier operations operating under 49 CFR 1546.101(a) or (b). The IFR establishes security procedures for aircraft operators and gateway airport operators, and security requirements relating to crewmembers, passengers, and armed security officers onboard aircraft operating into or out of DCA. Although this IFR is effective on August 18, 2005, an aircraft operator may not conduct operations into or out of DCA until it is determined by TSA to be in compliance with the security requirements set forth in this IFR.

**DATES:** This rule is effective August 18, 2005. Submit comments by September 19, 2005.

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

*Comments Filed Electronically:* You may submit comments through the docket Web site at <http://dms.dot.gov>. Please be aware that anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.).

You may review the applicable Privacy Act Statement published in the **Federal Register** on April 11, 2000 (65 FR 19477), or you may visit <http://dms.dot.gov>.

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

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

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

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

**FOR FURTHER INFORMATION CONTACT:** *For policy questions*, Robert Rottman, Office of Aviation Security Policy, Transportation Security Administration Headquarters, East Building, Floor 3, 601 12th Street, Arlington, VA 22202; telephone: (571) 227-2289; e-mail: [Robert.Rottman@dhs.gov](mailto:Robert.Rottman@dhs.gov).

*For questions related to Sensitive Security Information (SSI)*, Keith L. Moore, Director, SSI Program Office, Office of the Chief of Staff, Transportation Security Administration Headquarters, East Building, Floor 7, 601 12th Street, Arlington, VA 22202; telephone: (571) 227-3513; e-mail: [Keith.Moore1@dhs.gov](mailto:Keith.Moore1@dhs.gov).

*For legal questions*, Scott Houston, Office of Chief Counsel, Transportation Security Administration Headquarters, East Building, Floor 12, 601 12th Street, Arlington, VA 22202; telephone: (571) 227-3653; e-mail: [Scott.Houston@dhs.gov](mailto:Scott.Houston@dhs.gov).

**SUPPLEMENTARY INFORMATION:**

**Comments Invited**

This IFR is being adopted without prior notice and prior public comment. However, to the maximum extent possible, operating components within DHS provide an opportunity for public comment on regulations issued without prior notice. Accordingly, TSA invites interested persons to participate in this rulemaking by submitting written comments, data, or views. TSA also invites comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking. See **ADDRESSES** above for information on where to submit comments.

Comments that include trade secrets, confidential commercial or financial information, or SSI should not be submitted to the public regulatory docket. Please submit such comments separately from other comments on the rule. Comments containing this type of information should be appropriately marked and submitted by mail to the individual(s) listed in **FOR FURTHER INFORMATION CONTACT** section. Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold them in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA receives a request to examine or copy this information, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's FOIA regulation found in 6 CFR part 5.

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

If you want TSA to acknowledge receipt of your comments on this rulemaking, include with your comments a self-addressed, stamped postcard on which the docket number

appears. We will stamp the date on the postcard and mail it to you.

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

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

#### Availability of Rulemaking Document

You may obtain an electronic copy using the Internet by—

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) Web page (<http://dms.dot.gov/search/>);

(2) Accessing the Government Printing Office's Web page at <http://www.gpoaccess.gov/fr/index.html>; or

(3) Visiting the TSA's Law and Policy Web page at <http://www.tsa.gov/public/index.jsp>.

In addition, copies are available by writing or calling any of the individuals in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

#### Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires TSA to comply with small entity requests for information or advice about compliance with statutes and regulations within TSA's jurisdiction. Any small entity that has a question regarding this document may contact the persons listed in the **FOR FURTHER INFORMATION CONTACT** section for information or advice. You can get further information regarding SBREFA on the Small Business Administration's Web page at [http://www.sba.gov/advo/laws/law\\_lib.html](http://www.sba.gov/advo/laws/law_lib.html).

#### Good Cause for Issuing Rule Without Prior Notice and Comment

TSA is issuing this IFR without prior notice and opportunity to comment pursuant to its authority under section 4(a) of the Administrative Procedure Act (APA) (5 U.S.C. 553(b)). This provision authorizes the agency to issue a rule without prior notice and opportunity to comment when the agency for good cause finds that those procedures are "impracticable, unnecessary, or contrary to the public interest."

General aviation and charter operations that are not under full

security programs have been prohibited from arriving at or departing from DCA since September 11, 2001. However, regularly scheduled, commercial air carrier operations that had been prohibited at DCA after September 11, 2001, have been restored through issuance of Notices to Airmen (NOTAMs) by the Federal Aviation Administration (FAA). The operators that have not been able to resume flights into and out of DCA have suffered economic hardship. Because the interim final rule establishes a voluntary program that will lift the suspension of general aviation operations for a segment of affected parties, thereby removing an existing restriction on their activities, TSA believes there will be little, if any, objection from these parties to immediate implementation of the interim final rule. Moreover, the economic hardship of the operators would be unnecessarily extended by a notice and comment rulemaking. Therefore, delaying implementation until after a notice and public comment period is unnecessary. If some affected parties believe that changes in the interim final rule are warranted, they will have the opportunity to comment on the rule, while other affected parties that are able take advantage of the benefits of the rule may do so without further delay. Therefore, in recognition of the need to begin to restore general aviation operations in a manner that will neither give rise to security risks, nor prolong the economic hardship to affected parties, TSA finds good cause to forgo prior notice and public comment in issuing the interim final rule.

As previously noted, TSA requests comment on all aspects of this rule and will modify the rule if warranted.

#### Abbreviations of Terms Used In This Document

ADIZ—Air Defense Identification Zone  
 ASOP—Armed Security Officer Program  
 ATSA—Aviation and Transportation Security Act  
 CHRC—Criminal history records check  
 DASSP—DCA Access Standard Security Program  
 DCA—Ronald Reagan Washington National Airport  
 DHS—Department of Homeland Security  
 FAA—Federal Aviation Administration  
 FAM—Federal Air Marshal  
 FAMS—Federal Air Marshal Service  
 FBI—Federal Bureau of Investigation  
 FBO—fixed base operator  
 FRZ—Flight Restricted Zone  
 LEOSA—Law Enforcement Officers Safety Act  
 NOTAM—Notice to Airmen

PCSSP—Private Charter Standard Security Program  
 SSI—Sensitive Security Information  
 TFR—Temporary Flight Restriction  
 TFSSP—Twelve-Five Standard Security Program  
 TSA—Transportation Security Administration

#### I. Background

##### A. Operations at DCA

After the September 11, 2001, terrorist attacks against four U.S. commercial aircraft resulting in the tragic loss of human life at the World Trade Center, the Pentagon, and in southwest Pennsylvania, the FAA immediately prohibited all aircraft operations within the territorial airspace of the U.S., with the exception of certain military, law enforcement, and emergency related aircraft operations. This general prohibition was lifted in part on September 13, 2001. In the Washington, DC metropolitan area, however, aircraft operations remained prohibited at all civil airports within a 25 nautical mile radius of the Washington DC Very High Frequency Omnidirectional Range/Distance Measuring Equipment (VOR/DME). This action was accomplished via the U.S. NOTAM system.<sup>1</sup>

Limited commercial air carrier operations were permitted to resume at DCA on October 4, 2001, and through a series of emergency air traffic rules issued by the FAA under 14 CFR 91.139 and NOTAMs that followed, other restrictions were eliminated. Currently operations to and from DCA by aircraft operators that hold a certificate under 14 CFR part 121 and operate under a full security program approved by TSA in accordance with 49 CFR 1544.101(a), or a foreign air carrier security program approved by TSA in accordance with 49 CFR 1546.101(a) or (b), are permitted under NOTAM 3/2126. Generally these are regularly scheduled, commercial, passenger operations. General aviation operations and other operations that are not under one of these security programs under part 1544 or 1546 are prohibited.

As a result of this prohibition, many operators and the businesses they serve have experienced economic hardship. According to estimates prepared by the DCA Fixed Based Operator,<sup>2</sup>

<sup>1</sup> NOTAMs are used by the FAA to notify pilots of important information, including airspace restrictions. The FAA issued several NOTAMs regarding the restricted airspace over the Washington, DC, metropolitan area. The current NOTAM restricting aircraft operations in the Washington, DC, Flight Restricted Zone is NOTAM 3/2126.

<sup>2</sup> A Fixed Base Operator is an airport-based commercial enterprise that provides support

approximately 660 general aviation and charter flights occurred per week prior to September 11, 2001. The majority of these were corporate aircraft accommodating business travelers in the Washington, DC, area.

It is important to resume these operations at DCA to permit these operators, their customers, and affected local businesses to recover from the adverse economic impacts brought on by the events of September 11, 2001. However, DCA is located in close proximity to critical Federal Government assets, infrastructure, and functions. Any aircraft arriving at or departing from DCA will fly very near several significant government office buildings and national monuments. It would take very little time for such aircraft to inflict serious damage to any number of buildings in Washington, DC, and the surrounding area. Such an event could occur so quickly that it may not be possible to prevent. Therefore it is necessary to balance the economic interests of operators against the legitimate governmental security risks that exist.

After discussions with the United States Secret Service, the Federal Air Marshal Service (FAMS), the Department of Defense, the Homeland Security Council, and other Federal agencies, it has been determined that the national security concerns surrounding operations at DCA can be addressed effectively by requiring operators to comply with the security procedures set forth in this IFR. Applying these procedures to operations arriving at and departing from DCA will help to protect the critical national assets in the Washington, DC area from an airborne terrorist act. TSA has consulted with the associations that represent the operators subject to this rule, and they understand the need for special procedures at DCA. These operators are prepared to undertake special security procedures in order to recommence operations at DCA.

#### B. Statutory Background

On November 19, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA),<sup>3</sup> which created TSA, and transferred civil aviation security functions from the FAA to TSA. TSA transferred the bulk of FAA's civil aviation security regulations (in Title 14, Code of Federal Regulations) to TSA (in Title 49, Code of Federal Regulations) in a separate rulemaking

services to aircraft operators, such as maintenance, overnight parking, fueling, and deicing.

<sup>3</sup>Pub. L. 107-71, November 19, 2001, 115 Stat. 597.

(see docket number TSA-2002-11602, 67 FR 8340, February 22, 2002).

On December 12, 2003, Congress enacted the Vision 100-Century of Aviation Reauthorization Act.<sup>4</sup> Section 823 of Vision 100 requires the Secretary of Homeland Security to develop a security plan to permit general aviation aircraft to resume operations into and out of DCA.

#### II. Summary of the Interim Final Rule

For affected aircraft operators to fly into and out of DCA, they must designate a security coordinator and adopt a DCA Access Standard Security Program (DASSP). As part of the DASSP, they must ensure that all flight crewmembers have undergone a fingerprint-based criminal history records check (CHRC). Once aircraft operators have complied with those requirements, they will be eligible to apply to the FAA for a reservation, and to TSA for authorization, to operate specific flights into and out of DCA.

To receive authorization for a flight, aircraft operators must have name-based threat assessments conducted by TSA on their flight crewmembers and passengers. They must carry an armed security officer who also must have a threat assessment conducted by TSA, as well as specialized training and authorization from TSA. The operators must have their last point of departure from a Fixed Base Operator (FBO)<sup>5</sup> that holds a security program issued by TSA at an airport designated by TSA (referred to in the IFR as a "gateway airport"). At each gateway airport, TSA will inspect the aircraft and will screen the passengers, their carry-on property, and property carried in the cargo hold of the aircraft, before it departs for DCA. The aircraft operator must also comply with all applicable FAA rules, including those rules for operating in the Flight Restricted Zone (FRZ).<sup>6</sup>

The aircraft operator must reimburse TSA for any costs associated with carrying out this subpart. These costs include \$15 for the threat assessment TSA will conduct for each passenger and crewmember whose information the aircraft operator submits to TSA as part of the flight approval process, and \$296 per round trip into and out of DCA to

<sup>4</sup>Pub. L. 108-176, December 12, 2003, 117 Stat. 2490.

<sup>5</sup>An FBO is an airport-based commercial enterprise that provides support services to aircraft operators, such as maintenance, overnight parking, fueling, and de-icing.

<sup>6</sup>The FRZ is an airspace ring centered on the Washington DC VOR/DME with a radius of approximately 15 nautical miles. In order to enter and operate in FRZ airspace, an operator must comply with certain access and security procedures implemented by FAA and TSA.

cover the costs of using TSA screening personnel and equipment at DCA and the gateway airports.

#### III. Discussion of the Interim Final Rule

##### A. Scope and Definitions

This IFR creates a new subpart B in part 1562 of Title 49 of the Code of Federal Regulations (CFR). Subpart B applies to FBOs located at DCA and the gateway airports. It also applies to all aircraft operations into or out of DCA that are conducted under subpart B. The IFR also applies to passengers, crewmembers, and armed security officers onboard aircraft operations operated in accordance with the IFR. Finally, the IFR applies to individuals designated as security coordinators by aircraft operators in accordance with the IFR.

Section 1562.21(b) provides that each person operating an aircraft into or out of DCA must comply with this subpart, with certain exceptions. The exceptions include (1) military, law enforcement, or medivac aircraft operating into or out of DCA; (2) Federal and State Government aircraft operating under an airspace waiver approved by TSA and authorized by FAA;<sup>7</sup> (3) all-cargo aircraft operations; and (4) passenger aircraft operations conducted under a full security program approved by TSA in accordance with 49 CFR 1544.101(a) or a foreign air carrier security program approved by TSA in accordance with 49 CFR 1546.101(a) or (b).

This IFR does not apply to operations into or out of any airports other than DCA and gateway airports. Similarly, this IFR does not alter or suspend other regulations that TSA has issued or may issue that apply to aircraft operations. Further, this IFR does not affect the FAA's rules for operating into DCA, such as its rules relating to the allocation of reservations under the High Density Rule (14 CFR part 93, subpart K) and the Perimeter Rule (14 CFR 93.253), which prohibits a nonstop commercial aircraft operation to DCA from an airport that is more than 1,250 miles away from DCA.<sup>8</sup>

The IFR specifies that any aircraft operation into or out of DCA under the IFR must be conducted in accordance

<sup>7</sup>TSA will continue to coordinate with FAA, which authorizes waivers into and out of DCA for these and other certain operations, including Elected Official Operations, Government Operations, and Special Operations, in accordance with established policy.

<sup>8</sup>Due to slot control restrictions under the High Density Rule and the need to limit traffic volume in the FRZ for security purposes, it is expected that unscheduled aircraft operations into and out of DCA will be capped at 4 per hour for 12 hours a day, for a total of 48 operations daily.

with the DASSP and any other TSA-approved security program that covers that operation. If any requirements of the DASSP conflict with the requirements of another TSA-approved security program, such as a Twelve-Five Standard Security Program (TFSSP) or Private Charter Standard Security Program (PCSSP), the aircraft operation into or out of DCA must be conducted in accordance with the requirements of the DASSP.

For purposes of the IFR, the following definitions apply:

“Armed Security Officer Program” is defined as the security program approved by TSA, in coordination with the FAMS, for armed security officers authorized to carry a firearm in accordance with the IFR.

“Crewmember” is defined as a person assigned to perform duty in an aircraft during flight time. This includes pilots and flight attendants, but does not include armed security officers authorized to carry a firearm in accordance with the IFR.

“DCA” is defined as Ronald Reagan Washington National Airport.

“DASSP” (DCA Access Standard Security Program) is defined as the aircraft operator security program approved by TSA under part 1562 for aircraft operations into and out of DCA.

“FBO” is defined as a fixed base operator that has been approved by TSA under part 1562 to serve as a last point of departure for flights into or out of DCA. The approved FBOs are located at either DCA or one of the gateway airports.

“FBO Security Program” is defined as the security program approved by TSA under part 1562 for FBOs to serve flights into or out of DCA.

“Flightcrew member” is defined as a pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time. This is the same definition provided under 49 CFR 1540.5.

“Gateway airport” is defined as an airport that has been approved by TSA as a last point of departure for flights into DCA. More information on the gateway airports is provided below.

“Passenger” is defined as any person other than a flightcrew member on an aircraft. A “passenger” includes armed security officers authorized to carry a firearm in accordance with the rule.

#### *B. Aircraft Operator Requirements*

To operate into or out of DCA under part 1562, an aircraft operator must comply with the following requirements.

#### 1. Security Coordinators

The aircraft operator must designate an individual as a security coordinator responsible for implementing the DASSP and other security requirements under the IFR. The aircraft operator must provide TSA with the security coordinator's contact information and availability in accordance with the DASSP.

The security coordinator must undergo a fingerprint-based criminal history records check (CHRC) that does not disclose that he or she has a disqualifying criminal offense as described in 49 CFR 1544.229(d).<sup>9</sup> The IFR provides that this requirement is met if a security coordinator has already undergone a fingerprint-based CHRC in accordance with 49 CFR 1542.209, 1544.229, or 1544.230, with his or her current employer. The security coordinator also must undergo a security threat assessment performed by TSA.

To initiate the CHRC, the security coordinator must submit his or her fingerprints and required information to a fingerprint collector approved by TSA. The collector will forward the information to TSA, and TSA will forward the information to the Federal Bureau of Investigation (FBI). The FBI will conduct the CHRC and send the results to TSA, and TSA will adjudicate the results to verify that the security coordinator does not have a disqualifying criminal offense described in 49 CFR 1544.229(d). This process is similar to the process used for aircraft operators with a Twelve-Five Standard Security Program (TFSSP) or a Private Charter Standard Security Program (PCSSP).

If TSA informs the security coordinator that the CHRC discloses a disqualifying offense, he or she may seek to correct the record in accordance with the procedures set forth in 49 CFR 1544.229(h) and (i) regarding notification and correction of records. These procedures require an aircraft operator to notify an applicant when the applicant's FBI record discloses information that would disqualify the applicant, and provide the applicant with a copy of the FBI record if the applicant requests it. The applicant may contact the local jurisdiction responsible for the information in the record and the FBI to complete or correct the information, provided that the applicant notifies the aircraft

operator in writing, within 30 days of receiving notification that the applicant's FBI record discloses a disqualifying criminal offense, of his or her intent to correct the record. TSA notes that the procedures set forth in 49 CFR 1544.229(h) and (i) apply to the aircraft operator. Since TSA will be adjudicating the CHRC results for security coordinators under this IFR, TSA will perform the functions required of aircraft operators by 49 CFR 1544.229(h) and (i).

For purposes of the security threat assessment, the security coordinator must submit to TSA: his or her (1) legal name, including first, middle, and last; any applicable suffix, and any other names used; (2) current mailing address, including residential address if different than current mailing address; (3) date and place of birth; (4) citizenship status and date of naturalization if the individual is a naturalized citizen of the United States; and (5) alien registration number, if applicable. The security operator also may voluntarily provide his or her social security number. Using that information, TSA will conduct a security threat assessment and inform the aircraft operator of the results. If TSA determines that the security coordinator may pose a security threat, the aircraft operator may not designate the individual as a security coordinator. Failure to provide the social security number may result in delays in processing the application. Failure to provide the other information may result in the applicant being denied the request to serve as a security coordinator.

#### 2. DCA Access Standard Security Program (DASSP)

The aircraft operator must adopt and carry out the DASSP. To receive the DASSP, an aircraft operator must contact TSA through TSA's Office of Aviation Programs and request the DASSP. TSA will verify that the aircraft operator is a valid operator and then provide the aircraft operator with a non-disclosure agreement that the aircraft operator must sign, as the DASSP contains sensitive security information (SSI) that must be protected in accordance with TSA's SSI regulation at 49 CFR part 1520. TSA then will provide the DASSP to the aircraft operator. Once the aircraft operator implements the requirements of the DASSP, the aircraft operator must notify TSA. TSA will then inspect the aircraft operator to ensure that the program requirements have been implemented in accordance with the DASSP. Upon a satisfactory inspection, the aircraft operator will be eligible to apply to TSA

<sup>9</sup>These are the same disqualifying crimes used for TSA screeners, individuals with unescorted access to secured areas of an airport, and crewmembers employed by an aircraft operator operating under a TFSSP or PCSSP.

for approval to operate flights into and out of DCA in accordance with the requirements in the IFR, explained in further detail below.

### 3. Flightcrew Members

The aircraft operator must ensure that each flightcrew member<sup>10</sup> who will be assigned to an aircraft operating into or out of DCA complies with the requirements of the IFR. Each flightcrew member must undergo a fingerprint-based CHRC, using the same process and list of disqualifying criminal offenses used for the designated security coordinator. If a flightcrew member is informed that the CHRC discloses a disqualifying offense, he or she also may seek to correct the record in the same manner as the designated security coordinator. The IFR provides that the CHRC requirement is met if a flightcrew member has already undergone a fingerprint-based CHRC in accordance with 49 CFR 1542.209, 1544.229, or 1544.230, with his or her current employer.

Each flightcrew member also must undergo a check of their FAA record. A flightcrew member may not have a record on file with the FAA of a violation of: (1) A prohibited area designated under 14 CFR part 73; (2) a flight restriction established under 14 CFR 91.141 (flight restrictions in the proximity of the President and certain other parties); (3) special security instructions issued under 14 CFR 99.7 (air defense identification zone or defense area); (4) a restricted area designated under 14 CFR part 73; (5) emergency air traffic rules issued under 14 CFR 91.139 (emergency conditions); (6) a temporary flight restriction designated under 14 CFR 91.137 (vicinity of a disaster or hazard area), 91.138 (national disaster area in the State of Hawaii), or 91.145 (management of aircraft operations in the vicinity of aerial demonstrations and major sporting events); or (7) an area designated under 14 CFR 91.143 (flight limitations in the proximity of space flight operations). These violations also are considered disqualifying for pilots who apply for approval to operate to and from the Maryland Three Airports, which are located in the FRZ.<sup>11</sup>

### 4. Flight Approvals

The aircraft operator must apply for and receive a reservation from the FAA and authorization from TSA for each

flight into and out of DCA.<sup>12</sup> The aircraft operator first must apply to the FAA for assignment of a tentative reservation to operate into and/or out of DCA. The FAA will produce a tentative reservation based on air traffic scheduling and other relevant factors.

Then the aircraft operator must apply for TSA authorization for the flight by submitting to TSA the following information at least 24 hours prior to aircraft departure: (1) For each passenger and crewmember (both flightcrew and cabin crew) on the aircraft: legal name, including first, middle, and last; any applicable suffix, and any other names used; current mailing address, including residential address if different than current mailing address; date and place of birth; citizenship status and date of naturalization if the individual is a naturalized citizen of the United States; and alien registration number, if applicable; (2) the registration number of the aircraft; (3) the flight plan; and (4) any other information required by TSA.<sup>13</sup> TSA will conduct a name-based security threat assessment for each passenger and crewmember. If TSA notifies the aircraft operator that a passenger or crewmember may pose a security threat, the aircraft operator must ensure that the passenger or crewmember does not board the aircraft. TSA's ability to conduct a security threat assessment will be facilitated by the use of social security numbers and asks that passengers and crew consider voluntarily submitting social security numbers to TSA. Failure to provide the social security number may result in delays in processing the application. Failure to provide the other information may result in the applicant being denied the request to be a passenger or crewmember.

If TSA authorizes the flight, TSA will transmit its authorization to the FAA for assignment of a final reservation to operate into or out of DCA. Once FAA assigns the reservation, TSA will notify the aircraft operator.

The IFR specifies that TSA may, at its discretion, cancel any or all flight approvals at any time without prior notice to the aircraft operator. For example, if the threat level in the Washington, D.C., area or in the vicinity

of any of the gateway airports is set at ORANGE or RED, TSA is likely to cancel any and all flight approvals into and out of DCA. The IFR also specifies that TSA may, at its discretion, permit a flight to or from DCA to deviate from the requirements of the IFR, if TSA finds that such action would not be detrimental to transportation security or the safe operation of the aircraft. TSA will consult with the U.S. Secret Service, FAMS, Department of Defense, FAA, and other relevant government agencies prior to approving a flight to deviate from the requirements of the IFR. Finally, the IFR provides that TSA may, at its discretion, require any flight into or out of DCA under this subpart to comply with additional security measures. For instance, for certain operations, such as those with a large number of persons on board, TSA may require additional armed security officers onboard the aircraft.

### 5. Operating Requirements

For each flight into and out of DCA, an aircraft operator must comply with the following operating requirements specified in the IFR. The aircraft operator must ensure that each flight into DCA departs from a gateway airport and makes no intermediate stops before arrival at DCA. More information on the gateway airports is provided below.

The aircraft operator must ensure that the aircraft has been searched in accordance with the DASSP, and that each passenger and crewmember and all accessible property and property in inaccessible cargo holds on the aircraft has been screened in accordance with the DASSP prior to boarding the aircraft. TSA personnel will conduct the aircraft searches and screening of passengers, crewmembers, and property. The aircraft operator must ensure that each passenger and crewmember on the aircraft provides TSA screening personnel with a valid government-issued picture identification. If the aircraft is equipped with a cockpit door, the aircraft operator must ensure that the door is closed and locked at all times during the operation of the aircraft to or from DCA, unless FAA regulations require the door to remain open.<sup>14</sup> The aircraft operator must notify the National Capital Region Coordination Center prior to departure of the aircraft from a gateway airport or DCA.

The aircraft operator must ensure that each aircraft operating into or out of DCA has onboard at least one armed security officer who meets the

<sup>10</sup> These requirements do not apply to cabin crewmembers.

<sup>11</sup> See 70 FR 7150, February 10, 2005.

<sup>12</sup> As noted above, we expect that the total number of takeoff and landing reservations at DCA under the IFR will be limited to 48 per day.

<sup>13</sup> The aircraft operator is required to submit the required information for each passenger and crewmember only once per round trip flight. If any passengers or crewmembers are added on the flight out of DCA, the aircraft operator must submit the required information for those individuals at least 24 hours prior to the aircraft departing DCA.

<sup>14</sup> TSA notes that FAA regulations require that some cockpit doors remain open during takeoff and landing for safety reasons.

requirements specified in the IFR, which are discussed in greater detail below. For some flights, such as flights with a large number of passengers, TSA may require more than one armed security officer to be onboard the aircraft. In addition, if TSA or the FAMS requires that the aircraft have one or more Federal Air Marshals (FAMS) on board, the aircraft operator must allow the FAM(s) onboard, at no cost to the Federal Government.

The aircraft operator must ensure that the aircraft operates under instrument flight rules only. Finally, the aircraft operator must ensure that each passenger complies with any security measures mandated by TSA, and that no prohibited items are onboard the aircraft. TSA intends to use the same list of prohibited items that is currently used for regularly-scheduled commercial aircraft operations. In addition, as explained in greater detail below, TSA rules for aviation security, including the rules prohibiting interference with security measures and screening personnel and requiring individuals to submit to screening and inspection, will apply to passengers and crewmembers on aircraft operated into and out of DCA in accordance with the IFR.

#### 6. Costs

The aircraft operator must pay any costs and fees required under this part. As explained in greater detail below, the aircraft operator must pay a \$15 threat assessment fee for each passenger and crewmember whose information the aircraft operator submits to TSA as part of the flight approval process. In addition, the aircraft operator must reimburse TSA for additional costs TSA will incur in carrying out the requirements of the IFR.

On October 1, 2003, Congress enacted legislation directing TSA to collect reasonable fees to cover the costs of providing credentialing and background investigations in the transportation field.<sup>15</sup> Section 520 of the Department of Homeland Security Appropriations Act of 2004 (2004 Appropriations Act) authorizes TSA to collect fees to pay for the following costs: Conducting or obtaining a criminal history records check (CHRC); reviewing available law enforcement databases, commercial databases, and records of other governmental and international agencies; reviewing and adjudicating requests for waivers and appeals of TSA

decisions; and any other costs related to performing the background records check or providing the credential. Section 520 of the 2004 Appropriations Act mandates that any fee collected be available for expenditure only to pay for the costs incurred in providing services in connection with performing the background check or providing the credential. The fees collected shall remain available until expended.

Under the IFR, each aircraft operator must remit to TSA a fee of \$15 per person to defray the costs of the security threat assessment performed for passengers (including any armed security officers) and crewmembers on each flight operated into or out of DCA. The aircraft operator is required to pay this fee each time the aircraft operator submits the manifest to TSA for the required security threat assessments. In addition, each aircraft operator must reimburse TSA for the costs TSA incurs in carrying out the requirements of the IFR.

#### Population

The number of security threat assessments performed as a result of this IFR is drawn from general aviation industry data as well as TSA operational assumptions. The total figure is roughly equivalent to the product of two separate estimates: Total Round Trips Through DCA is the number of available general aviation slots divided by half (4 slots/hour  $\times$  12 hours/day  $\times$  365 days/year)/2 departures/round trip = 8,760), taking into account that round trips account for two allocated slots. This analysis assumes 100 percent capacity utilization of the available 48 daily slots, a premise based on pre-September 11, 2001, general aviation flight throughput of approximately 30,000 annual round trips through DCA. The second component is Average Persons Per Flight. Based on National Business Aviation Association (NBAA) analysis of pre-September 11, 2001, general aviation traffic at the airport, TSA has estimated that the Average Persons Per Flight is 6 persons (2 crewmembers and 4 passengers).<sup>16</sup> The product of these two numbers is 52,560 (8,760 round trips  $\times$  6 persons per flight).

#### Operational Assumptions

To develop its cost estimate, TSA has assumed the following procedures for general aviation flight authorizations and security threat assessments:

*Step 1:* An aircraft operator approved by TSA under the DASSP will apply to

the FAA for assignment of a tentative reservation to operate into and (typically) out of DCA. FAA will produce a tentative reservation based on air traffic scheduling availability and other relevant factors.

*Step 2:* The aircraft operator will apply to TSA for a flight approval and submit the names and other required information of all crewmembers and passengers.

*Step 3:* TSA will conduct name-checks against multiple government watch lists and other terrorist threat sources.

*Step 4:* Once TSA clears the crewmembers and passengers and approves the flight, TSA will transmit its approval to FAA for assignment of a final reservation to operate into and/or out of DCA.

*Step 5:* Once FAA assigns the final reservation, TSA will notify the aircraft operator.

*Step 6:* TSA will coordinate the aircraft operator's flight schedule with appropriate TSA field screening and inspection operations to perform physical screening at FBO operations at DCA or other gateway airports as required.

#### Cost Components

The following major cost components have been identified as required to perform the security threat assessment and requisite flight authorization functions. Each major component's cost estimates and supporting rationale and/or sources behind the estimate are discussed in detail below:

- Flight authorization automated system development ("Systems Costs")
- Federal authorization staff costs ("Program Staff Costs")
- Security threat assessment process costs ("Name Check Costs")

#### Systems Costs

To support up to 48 flights per day into and out of DCA (and all requisite information management of flight and applicant information), a Commercial Off-the-Shelf (COTS) software application will be required. Currently, TSA performs a similar processing function for other types of flight authorizations that cumulatively average some 400+ flight authorizations per week, or almost 23,000 flight authorizations per year. At present, TSA employs 9 full time employees (FTEs) to perform this labor-intensive process.

Rather than requiring significant numbers of additional personnel to handle the workload under this IFR, TSA intends to purchase an existing COTS application to automate much of the current flight authorization function

<sup>15</sup> Department of Homeland Security Appropriations Act, 2004, Section 520, Pub. L. 108-90, October 1, 2003, 117 Stat. 1156 (6 U.S.C. 469) (2004 Appropriations Act).

<sup>16</sup> According to the NBAA, over 90% of pre-September 11, 2001 general aviation traffic at DCA was corporate. A similar ratio is assumed for the current rollout.

at TSA, including operations into and out of DCA. Such a system is already operational and in use at the FAA. At a high level, the automated functionality and thus efficiency gained from such a system will be the following:

- Automation of applicant name, other biographical information, and flight information submission and transmission (rather than via fax and manual key entry of current waiver process).
- Automated applicant information submission to TSA's security threat assessment operations (versus fax/manual list management).
- Automated information exchange, including electronic signature for clearance documents and flight slotting, between TSA and FAA (versus current manual courier of documents daily between the two agencies).
- Automated tracking of flight volume/metrics, applicants and other performance metrics reporting capabilities as required.

TSA realizes that such a system will vastly improve not only the contemplated process for flight authorizations into and out of DCA, but also the efficiency and thus cost of the existing process for other flight authorizations. TSA notes that Section 520 of the Department of Homeland Security Appropriations Act, 2004, Pub. L. 107-90, 117 Stat. 1137 (Oct. 1, 2003) directs TSA to recover its costs related to providing a credential or performing background checks. As the flight authorization services are inextricably linked to providing the security threat

assessments under this program, TSA is including the cost of providing these services in the threat assessment fee.

TSA intends to charge aircraft operators operating into and out of DCA in accordance with the IFR only for those system costs equal to the proportion of total expected flight authorizations between the DCA program and all other flight authorization programs. TSA estimates that the acquisition, installation, and maintenance of a similar COTS application would total some \$4.1 million over a 5-year system and program lifecycle period. Thus, as the total annual flight authorization volume for general aviation operations at DCA is some 8,760 or 28 percent of the total annual expected volume of some 31,600 flight authorizations only 28 percent of the total 5-year system costs will be recovered in the fees charged under this IFR. The remaining 72 percent of system cost will become the responsibility of the existing flight authorization programs.

TSA will also incur several one-time technical "setup" costs, including an estimated \$100,000 to develop system interfaces with TSA systems for the security threat assessment, \$100,000 application installation and hosting setup charges, and an estimated \$100,000 for online fee payment functionality via the Federal Government's required electronic payment system for web-based payments, [www.pay.gov](http://www.pay.gov).

*Program Staff Costs*

Even with the reduction in manual labor TSA should realize with the automated flight authorization COTS system, TSA still estimates that 4 full time employees (FTEs) will be required to perform those functions that will not be automated. These functions are generally those that still require "live" communication and human judgment. This estimate also assumes that the 24-hour security threat assessment response time will necessitate some staffing during all 24 hours per day, 7 days per week. TSA has assumed annual staff cost for salary, benefits, and overhead of \$100,000 per employee.

*Name Check Costs*

TSA incurs both labor, system, and infrastructure/overhead costs each time it performs a name-based check against the multiple governmental watch lists and other terrorist threat sources. For the small portion of those names that are "hits" (names that match any of the various watch lists), TSA must perform identity verification and occasionally coordinate interagency law enforcement/apprehension activities. Based on TSA's operational history with other similar populations applying for clearance, and what it estimates the DCA general aviation population to require in terms of identity verification and other vetting operations, a \$2 per applicant security threat assessment cost has been derived. This fee is included in the \$15 security threat assessment fee described below.

TABLE 1.—5-YEAR LIFECYCLE COSTS  
[Program operating year]

	Year 1	Year 2	Year 3	Year 4	Year 5	Total
<i>Total Number of security threat assessments</i> .....	52,560	52,560	52,560	52,560	52,560	262,800
<i>Fixed Costs:</i>						
Automated Flight Authorization System .....	\$713,070	\$106,961	\$106,961	\$106,961	\$106,961	\$1,140,912
TSA Interface .....	100,000	0	0	0	0	100,000
Payment Interface .....	100,000	0	0	0	0	100,000
System Hosting Set-Up Costs .....	100,000	0	0	0	0	100,000
Scheduling Staff .....	400,000	400,000	400,000	400,000	400,000	2,000,000
<i>Total Fixed Costs</i> .....	1,513,070	506,961	506,961	506,961	506,961	3,440,912
<i>Variable Costs:</i>						
Name Checks .....	105,120	105,120	105,120	105,120	105,120	525,600
<i>Total Costs</i> .....	1,518,190	612,081	612,081	612,081	612,081	3,966,512

*Fee Summary*

Based on the costs and populations estimated above, TSA has calculated a fee of \$15 per person for the security threat assessments and requisite flight authorization services costs. To calculate the fee, TSA has amortized the

fixed costs of the security threat assessments over five years as this is generally accepted business practice for software and other infrastructure depreciation. The equation used to determine the fee is \$3,440,912 (fixed costs) + \$525,600 (variable costs over 5

years)/262,800 (5-year population of applicants) = \$15 per person.

Pursuant to the Chief Financial Officers Act of 1990, DHS and TSA are required to review these fees no less than every two years.<sup>17</sup> Upon review, if

<sup>17</sup> 31 U.S.C. 3512.



it is found that the fees are either too high (that is, total fees exceed the total cost to provide the services) or too low (that is, total fees do not cover the total costs to provide the services), TSA may propose changes to the fees. In addition, as DHS and TSA identify and implement additional efficiencies across numerous threat assessment and credentialing programs, any resulting cost savings will be incorporated into the fee levels accordingly.

In addition to the \$15 per person fee, the IFR requires each aircraft operator to pay TSA for the costs TSA expends in carrying out this subpart. These costs include the costs of using screening personnel and equipment at DCA and the gateway airports. These costs are currently estimated at \$296 per round trip into and out of DCA. TSA may revise these reimbursement cost figures if TSA determines that its estimated costs are too high or too low, and the reimbursable amounts may be modified periodically to reflect the most current costs of services provided.

All fees and reimbursement must be remitted to TSA in a form and manner approved by TSA, and TSA will not issue any refunds, unless a fee or reimbursement was paid in error. TSA will provide specific fee remittance instructions prior to enactment of the IFR. The IFR specifies that if an aircraft operator does not remit to TSA the fees and reimbursement required under the IFR, TSA may decline to process any requests for flight authorizations from the aircraft operator.

TSA notes that the aircraft operator or flightcrew member may also be required to pay a fee to any fingerprint collector for the fingerprint collection for crewmembers as well as the fee charged by the FBI for conducting a CHRC. In addition, the aircraft operator is responsible for paying to have a TSA qualified armed security officer onboard the aircraft.

#### 7. Protection of Sensitive Security Information

The aircraft operator must restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in 49 CFR part 1520, to persons with a need to know, and refer all requests for SSI by other persons to TSA. The IFR amends part 1520 to specify that the DASSP is SSI and that aircraft operators who receive the DASSP are covered persons under part 1520. Thus, aircraft operators subject to the IFR will be subject to the SSI protection requirements in part 1520. As explained further below, the IFR also amends part 1520 to cover FBOs and

armed security officers subject to part 1562.

#### 8. Other Security Procedures

The aircraft operator must comply with any additional security procedures required by TSA through order, Security Directive, or other means.

TSA notes that the following sections of 49 CFR part 1540 apply to persons involved with this program: § 1540.103, which prohibits certain fraud and intentional falsification; § 1540.105, which forbids certain interference with security measures; § 1540.107, which requires individuals to submit to screening and inspection; and § 1540.109, which prohibits persons from interfering with screening personnel. These sections apply throughout the TSA rules for aviation security (49 CFR chapter XII, subchapter C), and therefore now apply in the context of the requirements of part 1562.

In addition, this IFR amends § 1540.111 to apply to passengers on aircraft operated into and out of DCA under the DASSP. That section currently prohibits passengers from carrying weapons, explosives, and incendiaries on certain scheduled and charter flights, and is being expanded to also apply to passengers on aircraft operated into and out of DCA in accordance with the IFR and the DASSP.

#### 9. Compliance

The IFR requires an aircraft operator to permit TSA to conduct any inspections or tests, including copying records, to determine compliance with the IFR and the DASSP. The IFR also requires an aircraft operator, at the request of TSA, to provide evidence of compliance with the IFR and the DASSP, including copies of records.

The IFR specifies that noncompliance with the IFR or the DASSP may result in the cancellation of any and all of an aircraft operator's flight approvals and other enforcement action, as appropriate.

#### *B. Fixed Base Operator Requirements*

Each fixed base operator (FBO) from which flights into DCA operate under the IFR must adopt and carry out the FBO Security Program. TSA will provide the FBO Security Program to each participating FBO at DCA and the gateway airports. The gateway airports are: (1) Seattle-Tacoma, Washington; (2) Boston Logan, Massachusetts; (3) Houston Hobby, Texas; (4) White Plains, New York; (5) LaGuardia, New York; (6) Chicago Midway, Illinois; (7) Minneapolis-St. Paul, Minnesota; (8) West Palm Beach, Florida; (9) San

Francisco, California; (10) Teterboro, New Jersey; (11) Philadelphia, Pennsylvania; and (12) Lexington, Kentucky. TSA may revise or expand this list if necessary or appropriate.

TSA identified these airports as last points of departure for DCA based on volume and geographical reasons. Eight of the airports represent those that serviced the largest number of general aviation operations into DCA prior to September 11, 2001. Those airports are predominately centered in the northeast corridor where most DCA bound flights occur. The other airports are commercial service airports located throughout the U.S. that are in close proximity to general aviation airports that served DCA prior to September 11, 2001.

The FBO must designate a security coordinator who meets the same requirements as designated aircraft operator security coordinators. The security coordinator will be responsible for implementing the FBO Security Program and other security requirements required by the IFR. The FBO must provide TSA with the security coordinator's contact information and availability in accordance with the FBO Security Program.

The FBO must support the screening of persons and property, and the search of aircraft, in accordance with the requirements of the FBO Security Program.

The FBO must restrict the distribution, disclosure, and availability of SSI, as defined in 49 CFR part 1520, to persons with a need to know, and refer all requests for SSI by other persons to TSA. The IFR amends part 1520 to specify that the FBO Security Program is SSI and that FBOs that receive the FBO Security Program are covered persons under part 1520. Thus, FBOs subject to the IFR will be subject to the SSI protection requirements in part 1520.

The FBO must permit TSA to conduct any inspections or tests, including copying records, to determine compliance with this part and the FBO Security Program. In addition, at the request of TSA, the FBO must provide evidence of compliance with this part and the FBO Security Program, including copies of records.

#### *C. Armed Security Officer Requirements*

The IFR specifies the following requirements for security officers authorized to be armed onboard an aircraft operating into or out of DCA under a DASSP. Each armed security officer must comply with an Armed

Security Officer Program (ASOP) issued by TSA.

The armed security officer must be qualified to carry a firearm in accordance with the IFR. To be qualified, an armed security officer must be an active law enforcement officer, a retired law enforcement officer, or another individual who meets the requirements specified in the IFR.

A qualified active law enforcement officer is an employee of a governmental agency who: (1) Is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law; (2) has statutory powers of arrest; (3) is authorized by the agency to carry a firearm; (4) is not the subject of any disciplinary action by the agency; (5) is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and (6) is not prohibited by Federal law from receiving a firearm.

A qualified retired law enforcement officer is an individual who: (1) retired in good standing from service with a public agency as a law enforcement officer, other than for reasons of mental instability; (2) before such retirement, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest; (3) before such retirement, was regularly employed as a law enforcement officer for an aggregate of 15 years or more, or retired from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by such agency; (4) has a non-forfeitable right to benefits under the retirement plan of the agency; (5) is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and (6) is not prohibited by Federal law from receiving a firearm.

These requirements are consistent with the requirements specified for law enforcement officers and retired law enforcement officers under the Law Enforcement Officers Safety Act of 2004 (LEOSA).<sup>18</sup> LEOSA allows qualified law enforcement officers and qualified retired law enforcement officers to carry firearms in State and municipal jurisdictions beyond their own, but does not eliminate all restrictions that prohibit carrying firearms in certain areas or places, such as State or local government buildings and parks. Likewise, this law does not supersede or

affect Federal laws and regulations that restrict carriage of firearms in certain places, including 49 U.S.C. 46505 (criminal offense for carrying a weapon on aircraft) and the requirement to comply with all applicable provisions of 49 CFR 1544.219 (Carriage of Accessible Weapons) for a law enforcement officer to carry a firearm aboard a commercial aircraft. TSA notes that not all relevant jurisdictions have implemented the requirements of LEOSA, so some law enforcement officers and retired law enforcement officers may not yet be qualified under LEOSA. However, the requirements in this IFR are consistent with the requirements in LEOSA.

Under the IFR, TSA, in coordination with the FAMS, may authorize an individual other than an active or retired law enforcement officer to act as an armed security officer on an aircraft operating into or out of DCA, provided that they comply with the qualifications, threat assessment, training, and other requirements specified in the IFR. TSA, in coordination with the FAMS, is developing qualifications for individuals other than active and retired law enforcement officers, and will place them in the Aviation Security Officer Program. At a minimum, these individuals must not be under the influence of alcohol or another intoxicating or hallucinatory drug or substance and must not be prohibited by Federal law from receiving a firearm.

Each armed security officer must undergo a fingerprint-based CHRC that does not disclose that he or she has a criminal offense that would disqualify him or her from possessing a firearm under 18 U.S.C. 922(g). If an armed security officer is informed that the CHRC discloses a disqualifying offense, he or she may seek to correct the record in the same manner as a designated security coordinator or flightcrew member under the IFR.

Each armed security officer must submit to TSA his or her: (1) Legal name, including first, middle, and last; any applicable suffix, and any other names used; (2) current mailing address, including residential address if different than current mailing address; (3) date and place of birth; (4) citizenship status and date of naturalization if the individual is a naturalized citizen of the United States; and (5) alien registration number, if applicable. Armed security officers also are asked to voluntarily submit social security numbers to facilitate TSA's security threat assessment.

TSA will use that information to conduct a name-based security threat assessment. Each armed security officer

must undergo the name-based security threat assessment prior to receiving authorization from TSA and prior to boarding an aircraft operating into or out of DCA under a DASSP. If TSA notifies an aircraft operator that an armed security officer may pose a security threat, the aircraft operator may not use that armed security officer to comply with the requirements of the IFR. Failure to provide the social security number will result in delays in processing the application. Failure to provide the other information may result in the applicant being denied the request to serve as an armed security officer under this program.

Each armed security officer also must be authorized by TSA, in coordination with the FAMS, to carry a firearm under 49 U.S.C. 44903(d). That provision allows the Assistant Secretary of Homeland Security for TSA, with the approval of the Attorney General and the Secretary of State, to authorize individuals who carry out air transportation security duties to carry firearms and make arrests without warrant for any offense against the United States committed in the presence of the individual or for a felony under the laws of the United States, if the individual reasonably believes that the individual to be arrested has committed or is committing a felony.

Each armed security officer must have basic law enforcement training acceptable to TSA. The armed security officer also must complete a TSA-approved training course, developed in coordination with the FAMS, which will initially be provided by the Federal Government. Initially, this course will consist of such components as are germane to operating in this unique environment. However, TSA may augment this course with additional training in the future. The armed security officer will be required to pay for any costs associated with this training.

Each armed security officer must comply with an ASOP issued by TSA. The ASOP will contain instructions on the authorized use of force while onboard an aircraft operating into or out of DCA. Because the ASOP contains SSI, armed security officers must restrict the distribution, disclosure, and availability of the ASOP to persons with a need to know in accordance with 49 CFR part 1520, and refer all other requests for SSI by other persons to TSA.

The IFR authorizes an armed security officer approved by TSA to carry a firearm in accordance with the ASOP on an aircraft operating under a DASSP into or out of DCA, and to transport a firearm in accordance with the ASOP at

<sup>18</sup> Pub. L. 108-277, July 21, 2004.

any airport as needed to carry out duties under this subpart, including for travel to and from flights conducted under this subpart. It also authorizes an armed security officer approved by TSA to use force, including deadly force, in accordance with the ASOP.

The IFR prohibits an armed security officer onboard an aircraft operating into or out of DCA from consuming alcohol or using an intoxicating or hallucinatory drug or substance during the flight and within 8 hours prior to boarding the aircraft. The IFR requires each armed security officer onboard an aircraft operating into or out of DCA to carry a credential issued by TSA. The armed security officer must present the TSA-issued credential for inspection when requested by an authorized representative of TSA, FAA, the FAMS, the National Transportation Safety Board, any Federal, State, or local law enforcement officer, or any authorized aircraft operator representative. The armed security officer also must identify himself or herself to all crewmembers either personally or through another member of the crew before the flight. In addition, TSA and the FAMS may conduct random inspections of armed security officers, to ensure compliance with the ASOP.

Finally, the IFR provides that at the discretion of TSA, in coordination with the FAMS, the armed security officer's authorization under this part and 49 U.S.C. 44903(d) is suspended or withdrawn upon notification by TSA.

#### D. Implementation Schedule

TSA is planning to implement this program in two phases, and the program will be operational at the earliest date an aircraft operator is determined by TSA to be in compliance with the security requirements in this IFR. In Phase I, TSA expects to permit the following operations into and out of DCA:

- Operators under a partial security program approved by TSA under 49 CFR 1544.101(b), which operate aircraft with a passenger seating configuration of 31 or more but 60 or fewer seats.
- Operators under a PCSSP approved by TSA under 49 CFR 1544.101(f), which operate aircraft with a passenger seating configuration of 61 or more seats or a maximum certificated takeoff weight of 45,500 kg (100,309 pounds) or more.
- Operators in scheduled or charter service with a TFSSP approved by TSA under 49 CFR 1544.101(d), which operate aircraft with a maximum certificated takeoff weight of greater than 12,500 pounds.
- Aircraft operated by corporations.

TSA anticipates that approximately one year after implementing Phase I, the agency will evaluate the feasibility of Phase II, which may include the following operations:

- Aircraft operated by private persons.
- Scheduled and charter operations in aircraft not otherwise required to be under security programs (maximum certificated takeoff weight of 12,500 pounds or less).

In this way, the initial implementation will include those operators that tend to have more sophisticated operations and professional, experienced flight departments. These persons are likely to be most able to comply with the stringent security measures set out in this program. As TSA gains experience with this program and makes any adjustments found necessary, the agency will consider expanding the program to additional operators.

#### IV. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires Federal agencies to consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA section 3507(d), obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. This rulemaking contains information collection activities subject to the PRA. Accordingly, the following information requirements are being submitted to OMB as an emergency processing request for its review.

*Title:* Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations.

*Type of Request:* Emergency processing request of new collection.

*Summary:* Since September 11, 2001, general aviation aircraft operations have been prohibited at DCA. TSA is issuing this IFR to restore access to DCA for certain aircraft operations while maintaining the security of critical Federal Government and other assets in the Washington, DC Metropolitan Area. The IFR establishes security procedures for aircraft operators and gateway airport operators, and security requirements relating to crewmembers, passengers, and armed security officers onboard aircraft operating to or from DCA.

*Use of:* FBOs at DCA and the 12 gateway airports will be required to provide TSA with the fingerprints and identifying information of individuals designated as security coordinators in

accordance with the IFR. Aircraft operators that choose to operate into and out of DCA in accordance with the IFR will be required to provide TSA with fingerprints and identifying information of flightcrew members and individuals designated as security coordinators. TSA will use this information to perform a CHRC and a security threat assessment to determine if these individuals pose a security threat.

In addition, such aircraft operators will be required to provide TSA with identifying information for all crewmembers and passengers onboard each aircraft that operates into and out of DCA. TSA will use this information to perform security threat assessments in order to assess if the security coordinators, crewmembers, or passengers may pose a security threat.

Aircraft operators also will be required to provide TSA with the flight plan and registration number of any aircraft that operates to or from DCA. TSA will use this information to track and identify approved aircraft.

Armed security officers approved in accordance with the IFR will be required to provide TSA with fingerprints and identifying information. TSA will use this information to perform a CHRC and a threat assessment in order to assess whether the armed security officers pose a security threat.

*Respondents (including number of):* The likely respondents to this information collection requirement are general aviation passenger aircraft operators that operate into or out of DCA in accordance with the IFR, fixed base operators at DCA and the gateway airports, and armed security officers who apply for TSA approval in accordance with the IFR. TSA estimates that approximately 25 FBOs (one at DCA and two at each of the 12 gateway airports) will be willing to voluntarily participate in the FBO Security Program. TSA does not have current data on how many operators will be impacted by this rule. However, in the year preceding September 11, 2001, approximately 1,900 operators that would be subject to this rule flew into DCA. In that same time period, there were on average 660 flights per week involving these operators. However, the IFR limits the number of airports from which these operators can depart, and the number of takeoff and landing reservations at DCA is expected to be limited to 48 per day, so the total number of flights into DCA will undoubtedly be lower than the pre-2001 numbers. Accordingly, TSA assumes that the number of aircraft operators that

will apply for access to DCA will be significantly less than the number of aircraft operators that operated into and out of DCA prior to September 11, 2001.

TSA estimates that approximately 500 aircraft operators will apply for access to DCA and thus be required to respond to the information collection requirements. TSA estimates that approximately 1,500 armed security officers will apply for TSA approval in accordance with the IFR. Accordingly, TSA estimates the total number of respondents to be 2,025 (1,500 armed security officers + 500 aircraft operators + 25 FBOs).

*Frequency:* For security coordinators, armed security officers, and flightcrew members, the respondents will be required to provide the subject information only once for a CHRC. For passengers and crewmembers onboard aircraft operating into or out of DCA, the respondents will be required to provide the subject information for a name-based threat assessment for each flight into or out of DCA. TSA estimates the total number of responses to be 11,785 per year (500 aircraft operator security coordinator responses + 1,000 flightcrew member responses<sup>19</sup> + 25 FBO security coordinator responses + 1,500 armed security officer responses + 8,760 flight authorization responses).

*Annual Burden Estimate:* TSA estimates that it will take approximately 1 "hours to submit the required information, including fingerprints, for armed security officers, flightcrew members, and security coordinators, and approximately 1 hour to submit the required information for each flight into or out of DCA, for a total burden of 13,298 hours per year.

TSA is soliciting comments to—

(1) Evaluate whether the information collection requirements are necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

<sup>19</sup>TSA estimates that each aircraft operator will have 2 flightcrew members who will be required to submit fingerprints under the IFR.

(4) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Individuals and organizations may submit comments on the information collection requirements in this IFR by September 19, 2005, and should direct them via fax to the Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: DHS-TSA Desk Officer, at (202) 395-5806. Comments to OMB are most useful if received within 30 days of publication of the IFR.

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

#### V. Economic Analyses

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866, Regulatory Planning and Review (59 FR 51735, October 4, 1993), directs each Federal agency to 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 (5 U.S.C. 601, *et seq.*, as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, OMB directs agencies to assess the effect of regulatory changes on international trade. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1521-1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of \$100 million or more annually (adjusted for inflation).

#### A. Executive Order 12866 Assessment

Executive Order 12866, "Regulatory Planning and Review" (58 FR 51735, October 4, 1993) provides for making determinations whether a regulatory action is "significant" and therefore subject to OMB review and to the requirements of the Executive Order. Executive Order 12866 classifies a rule as significant if it meets any one of a number of specified conditions, including economic significance, which is defined as having an annual effect on the economy of \$100 million. A regulation is also considered a significant regulatory action if it raises novel legal or policy issues.

The Department concludes that while this action is not economically significant, it does raise novel legal and policy issues under Section 3(f)(4) of the Executive Order. Accordingly, this rulemaking has been reviewed by OMB as significant under Executive Order 12866.

TSA recognizes that the IFR may impose costs on some affected operators, which will stem from developing and implementing new security procedures for all flights into and out of DCA. However, the overall effect of the IFR, to permit these operators to resume DCA operations, may improve their economic condition. In any event, given the current security threat, TSA believes it is necessary to require these enhanced security measures.

Only FBOs at DCA and the gateway airports and general aviation aircraft operators desiring to resume operations to and from DCA will incur expenses. Each individual FBO and aircraft operator will evaluate the costs and benefits to them. FBOs and aircraft operators not realizing a benefit will not participate and will not incur any additional costs. The system-wide costs of this rule are approximately \$496 per flight. Average annual costs of \$8.7 million will be spread over a maximum of 17,520 flights based on the restriction of a total of 48 arrival/departure reservations at DCA per day. The following tables indicate the projected full and discounted costs, as well as the cost per flight.

## DCA GA COSTS

[2005 \$, millions]

Year	Equipment	LEOs	Threat assessment checks and infrastructure	Crew checks	Security coordinator: paperwork	Total cost
1 .....	\$1.038	\$6.721	\$1.518	\$0.024	\$0.9	\$10.2
2 .....	0.294	6.721	0.612	0.002	0.9	8.5
3 .....	0.294	6.721	0.612	0.002	0.9	8.5
4 .....	0.294	6.721	0.612	0.002	0.9	8.5
5 .....	0.294	6.721	0.612	0.002	0.9	8.5
6 .....	0.294	6.721	0.612	0.002	0.9	8.5
7 .....	0.294	6.721	0.612	0.002	0.9	8.5
8 .....	0.294	6.721	0.612	0.002	0.9	8.5
9 .....	0.294	6.721	0.612	0.002	0.9	8.5
10 .....	0.294	6.721	0.612	0.002	0.9	8.5
Total .....	3.681	67.210	7.027	0.046	8.8	87.0

## DC GA TOTAL COSTS

[Discounted \$, millions]

Year	Total cost	7% factor	7% discounted \$	3% factor	3% discounted \$
1 .....	\$10.20	1.000	\$10.20	1.000	\$10.20
2 .....	8.53	0.935	7.97	0.971	8.28
3 .....	8.53	0.873	7.45	0.943	8.04
4 .....	8.53	0.816	6.96	0.915	7.80
5 .....	8.53	0.763	6.51	0.888	7.57
6 .....	8.53	0.713	6.08	0.863	7.36
7 .....	8.53	0.666	5.68	0.837	7.14
8 .....	8.53	0.623	5.31	0.813	6.93
9 .....	8.53	0.582	4.96	0.789	6.73
10 .....	8.53	0.544	4.64	0.766	6.53
Total .....	86.96	.....	65.77	.....	76.60

## COST/FLIGHT

[2005 \$]

Year	Total cost	Flights	Av cost/flight
1 .....	\$10.20	17,520	\$582.23
2 .....	8.53	17,520	486.81
3 .....	8.53	17,520	486.81
4 .....	8.53	17,520	486.81
5 .....	8.53	17,520	486.81
6 .....	8.53	17,520	486.81
7 .....	8.53	17,520	486.81
8 .....	8.53	17,520	486.81
9 .....	8.53	17,520	486.81
10 .....	8.53	17,520	486.81
Total .....	86.96	175,200	496.35

Assumptions about unit costs are as follows: *1. Equipment*

Item	Unit cost	Quantity	Annual cost
ETD <sup>20</sup> Unit Purchase .....	\$41,500.00	25	\$1,037,500.00
Recurring:			
Maintenance: ETD .....	11,550.00	25	288,750.00
Misc. (Gloves, Batteries, etc.) .....	.....	.....	5,000.00
Total: Recurring Maintenance .....	.....	.....	293,750.00

<sup>20</sup> Explosives Trace Detection.

2. Armed Security Officers

Armed security officer hourly costs are computed at the wage rate for Bureau of Labor Statistics (BLS) figures for Police and detectives, public service Sheriffs, bailiffs, and other law enforcement officers, all United States, of \$21.11 grossed up for employer paid

taxes to \$24.55 per hour. The historical data does not reveal how many flights into and out of DCA were round trips, so \$122.38 average fare was allowed for a return trip. Wage costs were computed at an average 8 hour day, per diem calculated at the average Federal rate of \$31. The per-trip costs then average

\$350 × 17,520 flights = \$6.1 million per year. Training for the armed security officers is assumed at an average of 16 hours/year for 1,500 armed security officers for an additional \$589,000 per year.

3. Threat Assessment Checks and Infrastructure

NAME CHECK POPULATION AND COST

Round-trip flights = (24 flights/day × 365 days)	Number of checks = (4 passengers + 2 crew per flight)	Name based check unit cost	Total annual name based check cost
8,760	52,560	\$2	\$105,120

The number of round-trip flights into and out of DCA is equal to the number of slots per day (4 slots × 12 hours = 48) times the number of days in a year (365)

divided by two, which equals 8,760 round trip flights per year. Assuming that each flight has, on average, four passengers and two crew, there will be

52,560 name based threat assessments per year. The cost for running each check is \$2 which places the annual cost at \$105,120.

NAME BASED THREAT ASSESSMENT COST

[2005 \$, thousands]

Year	Automated flight authorization system	Threat assessment system interface	Payment processing and application setup	System hosting setup costs	Scheduling staff	Name based checks	Total
1 .....	\$713	\$100	\$100	\$100	\$400	\$105	\$1,518
2 .....	107	0	0	0	400	105	612
3 .....	107	0	0	0	400	105	612
4 .....	107	0	0	0	400	105	612
5 .....	107	0	0	0	400	105	612
6 .....	107	0	0	0	400	105	612
7 .....	107	0	0	0	400	105	612
8 .....	107	0	0	0	400	105	612
9 .....	107	0	0	0	400	105	612
10 .....	107	0	0	0	400	105	612
Total .....	1,676	100	100	100	4,000	1,051	7,027

The Automated Flight Authorization System is estimated to cost \$713,000 in initial development, which will be incurred in the first year. Every year thereafter, TSA estimates the system will cost \$106,961 for annual IT overhead and maintenance. The Threat Assessment Systems Interface, Payment Processing and Application Setup, and System Hosting Setup costs are only incurred in the first year. These reflect

various costs of making the system operational. TSA estimates that it will require 4 FTEs to operate the system. The fully loaded cost of one Federal employee is estimated at \$100,000 per year; therefore the staffing costs will be \$400,000 per year. The ten year total for the name based threat assessments is estimated to be \$7.027 million.

4. Flightcrew Member CHRCs

Although some flightcrew members will have had fingerprint-based CHRCs under other security programs, TSA assumed 500 flightcrew members would need CHRCs in the first year with a 10% per year replacement rate. At \$48 per CHRC this is \$24,000 for the first year and \$2,500 each additional year.

5. Security Coordinators and Paperwork

Item	Loaded hourly rate	Hours	Quantity	Total
Passenger and Crew Manifest and Security Program work .....	\$50.26	( <sup>1</sup> )	17,520	\$880,555.20
Initial Program and Inspection .....	50.26	8	13	5,227.04

<sup>1</sup> Average 1 hour/flight.

6. Benefits

The primary benefit of this IFR is that it provides access to DCA by general aviation aircraft operations that currently are prohibited. TSA believes that allowing general aviation aircraft operations to resume at DCA will relieve

some of the economic hardship these operators have suffered due to the current restrictions.

TSA believes that the IFR affords these benefits without decreasing the security of the vital government assets in the Washington, DC metropolitan

area. The security provisions contained in this IFR are an integral part of the effort to identify and defeat the threat posed by members of foreign terrorist groups to vital U.S. assets and security. The IFR requires general aviation aircraft operators to adopt and carry out

security measures that are comparable to the security measures required of regularly scheduled, commercial aircraft. TSA believes that the IFR will mitigate the risk that an airborne strike initiated from DCA, located moments away from vital national assets, will occur. TSA recognizes that such an impact may not cause substantial damage to property or a large structure. However, it could potentially result in an undetermined number of fatalities and injuries, as well as reduced tourism. The resulting tragedy would adversely impact the regional economies.

For these reasons, TSA has concluded that the benefits associated with the IFR justify its costs.

#### B. Regulatory Flexibility Act Assessment

TSA has not assessed whether this rule will have a significant economic impact on a substantial number of small entities, as defined in the Regulatory Flexibility Act. Under Executive Order 13272 and the Regulatory Flexibility Act, when an agency publishes a rulemaking without prior notice and opportunity for comment, the Regulatory Flexibility Act requirements do not apply. TSA is adopting this IFR without prior notice and opportunity for public comment. Therefore, no Regulatory Flexibility Act analysis is provided.

#### C. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as security, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. In addition, consistent with the Administration's belief in the general superiority and desirability of free trade, it is the policy of TSA to remove or diminish, to the extent feasible, barriers to international trade, including both barriers affecting the export of American goods and services to foreign countries and barriers affecting the import of foreign goods and services into the United States.

In accordance with the above statute and policy, TSA has assessed the potential effect of this IFR and has determined that it will impose the same costs on domestic and international entities, and thus will have a neutral trade impact.

#### D. Unfunded Mandates Assessment

The Unfunded Mandates Reform Act of 1995 (the Act), enacted as Pub. L. 104-4 on March 22, 1995, is intended to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of the Act requires each Federal agency to prepare a written statement that assesses the effect of any Federal mandate found in a rulemaking action that may result in an expenditure of \$100 million or more (adjusted annually for inflation) in any one year by State, local, and tribal governments, in the aggregate, or by the private sector. Such a mandate is identified as a "significant regulatory action." This IFR is not a significant regulatory action pursuant to the Act.

In addition, the Act does not apply to a regulatory action in which no notice of proposed rulemaking is published, as is the case in this proceeding. Accordingly, it is not necessary to prepare a statement under the Act.

#### VI. Executive Order 13132, Federalism

Executive Order 13132 requires TSA to develop an accountable process to ensure "meaningful and timely input by State and local officials in the development of regulatory policies that have federalism implications." "Policies that have federalism implications" are defined in the Executive Order to include regulations that have "substantial direct effects 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." Under the Executive Order, TSA may construe a Federal statute to preempt State law only where, among other things, the exercise of State authority conflicts with the exercise of Federal authority under the Federal statute.

TSA has analyzed this IFR under the principles and criteria of Executive Order 13132, Federalism. TSA has determined that this action will not have a substantial direct effect on the States, the relationship between the national government and the States, or the distribution of power and responsibilities among the various levels of government. Thus, TSA has determined that the IFR will not have sufficient Federalism implications to warrant the preparation of a Federal Assessment.

#### VII. Environmental Analysis

TSA has reviewed this action for purposes of the National Environmental Review Policy Act of 1969 (NEPA) (42 U.S.C. 4321-4347) and has determined

that this action will not have a significant effect on the human environment.

#### VIII. Energy Impact Analysis

TSA has assessed the energy impact of this IFR in accordance with the Energy Policy and Conservation Act (EPCA), Public Law 94-163, as amended (42 U.S.C. 6362). TSA has tentatively determined that this IFR will not be a major regulatory action under the provisions of the EPCA.

#### List of Subjects in 49 CFR Parts 1520, 1540, and 1562

Air traffic control, Aircraft, Airmen, Airports, Aviation safety, Screening, Security, Sensitive security information, Weapons.

#### The Amendments

■ For the reasons stated in the preamble, the Transportation Security Administration amends parts 1520, 1540, and 1562 of Title 49, Code of Federal Regulations, as follows:

#### PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

■ 1. The authority citation for part 1520 continues to read as follows:

**Authority:** 46 U.S.C. 70102-70106, 70117; 49 U.S.C. 114, 40113, 44901-44907, 44913-44914, 44916-44918, 44935-44936, 44942, 46105.

■ 2. In § 1520.3, revise the definition of "Security program" to read as follows:

#### § 1520.3 Terms used in this part.

\* \* \* \* \*

*Security program* means a program or plan and any amendments, developed for the security of the following, including any comments, instructions, or implementing guidance:

- (1) An airport, aircraft, or aviation cargo operation;
- (2) A fixed base operator;
- (3) A maritime facility, vessel, or port area; or
- (4) A transportation-related automated system or network for information processing, control, and communications.

\* \* \* \* \*

■ 3. In § 1520.5, revise paragraph (b)(1)(i) and add paragraph (b)(8)(iv) to read as follows:

#### § 1520.5 Sensitive security information.

\* \* \* \* \*

(b) \* \* \*

(1) \* \* \*

(i) Any aircraft operator, airport operator, or fixed base operator security

program, or security contingency plan under this chapter;

\* \* \* \* \*

(8) \* \* \*

(iv) Any armed security officer procedures issued by TSA under 49 CFR part 1562.

\* \* \* \* \*

■ 4. In § 1520.7, revise paragraph (a) to read as follows:

§ 1520.7 Covered persons.

(a) Each airport operator, aircraft operator, and fixed base operator subject to the requirements of subchapter C of this chapter, and each armed security officer under subpart B of part 1562.

\* \* \* \* \*

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

■ 5. The authority citation for part 1540 continues to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

Subpart B—Responsibilities of Passengers and Other Individuals and Persons

■ 6. In § 1540.111, revise paragraphs (a)(3), (b)(2), and (c) to read as follows:

§ 1540.111 Carriage of weapons, explosives, and incendiaries by individuals.

(a) \* \* \*

(3) When the individual is attempting to board or onboard an aircraft for which screening is conducted under §§ 1544.201, 1546.201, or 1562.23 of this chapter.

(b) \* \* \*

(2) An individual authorized to carry a weapon in accordance with §§ 1544.219, 1544.221, 1544.223, 1546.211, or subpart B of part 1562 of this chapter.

\* \* \* \* \*

(c) In checked baggage. A passenger may not transport or offer for transport in checked baggage or in baggage carried in an inaccessible cargo hold under § 1562.23 of this chapter:

(1) Any loaded firearm(s).

(2) Any unloaded firearm(s) unless—

- (i) The passenger declares to the aircraft operator, either orally or in writing, before checking the baggage, that the passenger has a firearm in his or her bag and that it is unloaded;
(ii) The firearm is unloaded;
(iii) The firearm is carried in a hard-sided container; and

(iv) The container in which it is carried is locked, and only the passenger retains the key or combination.

(3) Any unauthorized explosive or incendiary.

\* \* \* \* \*

■ 7. Revise the title of part 1562 to read as follows:

PART 1562—OPERATIONS IN THE WASHINGTON, DC, METROPOLITAN AREA

■ 8. The authority citation for part 1562 is revised to read as follows:

Authority: 49 U.S.C. 114, 40114, Sec. 823, Pub. L. 108–176, 117 Stat. 2595.

■ 9. Add a new subpart B to read as follows:

Subpart B—Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations

Sec.

1562.21 Scope, general requirements, and definitions.

1562.23 Aircraft operator and passenger requirements.

1562.25 Fixed base operator requirements.

1562.27 Costs.

1562.29 Armed security officer requirements.

Subpart B—Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations

§ 1562.21 Scope, general requirements, and definitions.

(a) Scope. This subpart applies to aircraft operations into or out of Ronald Reagan Washington National Airport (DCA), fixed base operators located at DCA or gateway airports; individuals designated as a security coordinator by aircraft operators or fixed base operators; and crewmembers, passengers, and armed security officers on aircraft operations subject to this subpart.

(b) General requirements. Each person operating an aircraft into or out of DCA must comply with this subpart, except:

(1) Military, law enforcement, and medivac aircraft operations;

(2) Federal and State government aircraft operations operating under an airspace waiver approved by TSA and the Federal Aviation Administration;

(3) All-cargo aircraft operations;

(4) Passenger aircraft operations conducted under:

(i) A full security program approved by TSA in accordance with 49 CFR 1544.101(a); or

(ii) A foreign air carrier security program approved by TSA in accordance with 49 CFR 1546.101(a) or (b).

(c) Other security programs. Each aircraft operator required to comply with this subpart for an aircraft

operation into or out of DCA must also comply with any other TSA-approved security program that covers that operation. If any requirements of the DASSP conflict with the requirements of another TSA-approved security program, the aircraft operation must be conducted in accordance with the requirements of the DASSP.

(d) Definitions. For purposes of this subpart, the following definitions apply:

Armed Security Officer Program means the security program approved by TSA, in coordination with the Federal Air Marshal Service, for security officers authorized to carry a firearm under § 1562.29 of this part.

Crewmember means a person assigned to perform duty in an aircraft during flight time. This does not include an armed security officer.

DCA means Ronald Reagan Washington National Airport.

DASSP means the aircraft operator security program (DCA Access Standard Security Program) approved by TSA under this part for aircraft operations into and out of DCA.

FBO means a fixed base operator that has been approved by TSA under this part to serve as a last point of departure for flights into or out of DCA.

FBO Security Program means the security program approved by TSA under this part for FBOs to serve flights into or out of DCA.

Flightcrew member means a pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time.

Gateway airport means an airport that has been approved by TSA under this part as a last point of departure for flights into DCA under this part.

Passenger means any person on an aircraft other than a flightcrew member. A “passenger” includes an armed security officer authorized to carry a firearm in accordance with the rule.

§ 1562.23 Aircraft operator and passenger requirements.

(a) General. To operate into or out of DCA, an aircraft operator must:

(1) Designate a security coordinator responsible for implementing the DASSP and other security requirements required under this section, and provide TSA with the security coordinator’s contact information and availability in accordance with the DASSP.

(2) Adopt and carry out the DASSP.

(3) Ensure that each crewmember of an aircraft operating into or out of DCA meets the requirements of paragraph (c) of this section.

(4) Apply for and receive a reservation from the Federal Aviation Administration and authorization from



TSA for each flight into and out of DCA in accordance with paragraph (d) of this section.

(5) Comply with the operating requirements in paragraph (e) of this section for each flight into and out of DCA.

(6) Pay any costs and fees required under this part.

(7) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know, and refer all requests for SSI by other persons to TSA.

(8) Comply with any additional security procedures required by TSA through order, Security Directive, or other means.

(b) *Security coordinator.* Each security coordinator designated by an aircraft operator under paragraph (a) of this section:

(1) Must undergo a fingerprint-based criminal history records check that does not disclose that he or she has a disqualifying criminal offense as described in § 1544.229(d) of this chapter. This standard is met if the security coordinator is in compliance with the fingerprint-based criminal history records check requirements of §§ 1542.209, 1544.229, or 1544.230 of this chapter with his or her current employer.

(2) Must submit to TSA his or her:

(i) Legal name, including first, middle, and last; any applicable suffix, and any other names used.

(ii) Current mailing address, including residential address if different than current mailing address.

(iii) Date and place of birth.

(iv) Social security number, (submission is voluntary, although recommended).

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

(vi) Alien registration number, if applicable.

(3) Must successfully complete a TSA security threat assessment.

(4) May, if informed that a disqualifying offense has been disclosed, correct the record in accordance with the procedures set forth in paragraphs (h) and (i) of § 1544.229 of this chapter regarding notification and correction of records.

(c) *Flightcrew member requirements.* Each flightcrew member of an aircraft, as defined in 49 CFR 1540.5, operating into or out of DCA:

(1) Must undergo a fingerprint-based criminal history records check that does not disclose that he or she has a disqualifying criminal offense as

described in § 1544.229(d) of this chapter. This standard is met if the flightcrew member is in compliance with the fingerprint-based criminal history records check requirements of §§ 1542.209, 1544.229, or 1544.230 of this chapter with his or her current employer.

(2) Must not have a record on file with the Federal Aviation Administration of a violation of—

(i) A prohibited area designated under 14 CFR part 73;

(ii) A flight restriction established under 14 CFR 91.141;

(iii) Special security instructions issued under 14 CFR 99.7;

(iv) A restricted area designated under 14 CFR part 73;

(v) Emergency air traffic rules issued under 14 CFR 91.139;

(vi) A temporary flight restriction designated under 14 CFR 91.137, 91.138, or 91.145; or

(vii) An area designated under 14 CFR 91.143.

(3) May, if informed that a disqualifying offense has been disclosed, correct the record in accordance with the procedures set forth in paragraphs (h) and (i) of § 1544.229 of this chapter regarding notification and correction of records.

(d) *Flight authorization requirements.* To receive authorization to operate an aircraft into or out of DCA, an aircraft operator must follow the procedures in this paragraph.

(1) The aircraft operator must apply to the Federal Aviation Administration for a tentative reservation, in a form and manner approved by the Federal Aviation Administration.

(2) The aircraft operator must submit to TSA, in a form and manner approved by TSA, the following information at least 24 hours prior to aircraft departure:

(i) For each passenger and crewmember on the aircraft:

(A) Legal name, including first, middle, and last; any applicable suffix, and any other names used.

(B) Current mailing address, including residential address if different than current mailing address.

(C) Date and place of birth.

(D) Social security number, (submission is voluntary, although recommended).

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

(F) Alien registration number, if applicable.

(ii) The registration number of the aircraft.

(iii) The flight plan.

(iv) Any other information required by TSA.

(3) TSA will conduct a name-based security threat assessment for each passenger and crewmember. If TSA notifies the aircraft operator that a passenger or crewmember may pose a security threat, the aircraft operator must ensure that the passenger or crewmember does not board the aircraft before the aircraft departs out of DCA or out of a gateway airport to DCA.

(4) If TSA approves the flight, TSA will transmit such approval to the Federal Aviation Administration for assignment of a final reservation to operate into or out of DCA. Once the Federal Aviation Administration assigns the final reservation, TSA will notify the aircraft operator.

(5) TSA may, at its discretion, cancel any or all flight approvals at any time without prior notice to the aircraft operator.

(6) TSA may, at its discretion, permit a flight into or out of DCA to deviate from the requirements of this subpart, if TSA finds that such action would not be detrimental to transportation security or the safe operation of the aircraft.

(7) TSA may, at its discretion, require any flight into or out of DCA under this subpart to comply with additional security measures.

(e) *Operating requirements.* Each aircraft operator must:

(1) Ensure that each flight into DCA departs from a gateway airport and makes no intermediate stops before arrival at DCA.

(2) Ensure that each passenger and crewmember on an aircraft operating into or out of DCA has been screened in accordance with the DASSP prior to boarding the aircraft.

(3) Ensure that all accessible property and property in inaccessible cargo holds on an aircraft operating into or out of DCA has been screened in accordance with the DASSP prior to boarding the aircraft.

(4) Ensure that each aircraft operating into or out of DCA has been searched in accordance with the DASSP.

(5) Ensure that each passenger and crewmember on an aircraft operating into or out of DCA provides TSA with a valid government-issued picture identification in accordance with the DASSP.

(6) If the aircraft operating into or out of DCA is equipped with a cockpit door, ensure that the door is closed and locked at all times during the operation of the aircraft to or from DCA, unless Federal Aviation Administration regulations require the door to remain open.

(7) Ensure that each aircraft operating into or out of DCA has onboard at least one armed security officer who meets

the requirements of § 1562.29 of this chapter. This requirement does not apply if—

(i) There is a Federal Air Marshal onboard; or

(ii) The aircraft is being flown without passengers into DCA to pick up passengers, or out of DCA after deplaning all passengers.

(8) Ensure that an aircraft operating into or out of DCA has any Federal Air Marshal onboard, at no cost to the Federal Government, if TSA or the Federal Air Marshal Service so requires.

(9) Notify the National Capital Region Coordination Center prior to departure of the aircraft from DCA or a gateway airport.

(10) Ensure that each aircraft operating into or out of DCA operates under instrument flight rules.

(11) Ensure that each passenger complies with any security measures mandated by TSA.

(12) Ensure that no prohibited items are onboard the aircraft.

(f) *Compliance.* (1) Each aircraft operator must:

(i) Permit TSA to conduct any inspections or tests, including copying records, to determine compliance with this part and the DASSP.

(ii) At the request of TSA, provide evidence of compliance with this part and the DASSP, including copies of records.

(2) Noncompliance with this part or the DASSP may result in the cancellation of an aircraft operator's flight approvals and other remedial or enforcement action, as appropriate.

(g) *Passenger requirements.* Each passenger, including each armed security officer, who boards or attempts to board an aircraft under this section must:

(1) Provide information to the aircraft operator as provided in this section.

(2) Provide to TSA upon request a valid government-issued photo identification.

(3) Comply with security measures as conveyed by the aircraft operator.

(4) Comply with all applicable regulations in this chapter, including § 1540.107 regarding submission to screening and inspection, § 1540.109 regarding prohibition against interference with screening personnel, and § 1540.111 regarding carriage of weapons, explosives, and incendiaries by individuals.

#### § 1562.25 Fixed base operator requirements.

(a) *Security program.* Each FBO must adopt and carry out an FBO Security Program.

(b) *Screening and other duties.* Each FBO must—

(1) Designate a security coordinator who meets the requirements in § 1562.23(b) of this part and is responsible for implementing the FBO Security Program and other security requirements required under this section, and provide TSA with the security coordinator's contact information and availability in accordance with the FBO Security Program.

(2) Support the screening of persons and property in accordance with the requirements of this subpart and the FBO Security Program.

(3) Support the search of aircraft in accordance with the requirements of this subpart and the FBO Security Program.

(4) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know, and refer all requests for SSI by other persons to TSA.

(5) Perform any other duties required under the FBO Security Program.

(c) *Compliance.* (1) Each FBO must:

(i) Permit TSA to conduct any inspections or tests, including copying records, to determine compliance with this part and the FBO Security Program.

(ii) At the request of TSA, provide evidence of compliance with this part and the FBO Security Program, including copies of records.

(2) Noncompliance with this part or the FBO Security Program may result in the cancellation of an aircraft operator's flight approvals and other remedial or enforcement action, as appropriate.

#### § 1562.27 Costs.

(a) Each aircraft operator must pay a threat assessment fee of \$15 for each passenger and crewmember whose information the aircraft operator submits to TSA in accordance with § 1562.23(d) of this part.

(b) Each aircraft operator must pay to TSA the costs associated with carrying out this subpart, as provided in its DASSP.

(c) All fees and reimbursement must be remitted to TSA in a form and manner approved by TSA.

(d) TSA will not issue any refunds, unless any fees or reimbursement funds were paid in error.

(e) If an aircraft operator does not remit to TSA the fees and reimbursement funds required under this section, TSA may decline to process any requests for authorization from the aircraft operator.

#### § 1562.29 Armed security officer requirements.

(a) *General.* Unless otherwise authorized by TSA, each armed security officer must meet the following requirements:

(1) Be qualified to carry a firearm in accordance with paragraph (b) of this section.

(2) Successfully complete a TSA security threat assessment as described in paragraph (c) of this section.

(3) Meet such other requirements as TSA, in coordination with the Federal Air Marshal Service, may establish in the Armed Security Officer Security Program.

(4) Be authorized by TSA, in coordination with the Federal Air Marshal Service, under 49 U.S.C. 44903(d).

(b) *Qualifications.* To be qualified to carry a firearm under this subpart, an individual must meet the requirements in paragraph (1), (2), or (3) of this section, unless otherwise authorized by TSA, in coordination with the Federal Air Marshal Service.

(1) *Active law enforcement officers.* An active law enforcement officer must be an employee of a governmental agency who—

(i) Is authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law;

(ii) Has statutory powers of arrest;

(iii) Is authorized by the agency to carry a firearm;

(iv) Is not the subject of any disciplinary action by the agency;

(v) Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(vi) Is not prohibited by Federal law from receiving a firearm.

(2) *Retired law enforcement officers.* A retired law enforcement officer must be an individual who—

(i) Retired in good standing from service with a public agency as a law enforcement officer, other than for reasons of mental instability;

(ii) Before such retirement, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest;

(iii) Before such retirement, was regularly employed as a law enforcement officer for an aggregate of 15 years or more, or retired from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by such agency;

(iv) Has a non-forfeitable right to benefits under the retirement plan of the agency;

(v) Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(vi) Is not prohibited by Federal law from receiving a firearm.

(3) *Other individuals.* Any other individual must—

(i) Meet qualifications established by TSA, in coordination with the Federal Air Marshal Service, in the Armed Security Officer Program;

(ii) Not be under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

(iii) Not be prohibited by Federal law from receiving a firearm.

(c) *Threat assessments.* To be authorized under this section, each armed security officer:

(1) Must undergo a fingerprint-based criminal history records check that does not disclose that he or she has a criminal offense that would disqualify him or her from possessing a firearm under 18 U.S.C. 922(g).

(2) May, if informed that a disqualifying offense has been disclosed, correct the record in accordance with the procedures set forth in paragraphs (h) and (i) of § 1544.229 of this chapter regarding notification and correction of records.

(3) Must submit to TSA his or her:

(i) Legal name, including first, middle, and last; any applicable suffix, and any other names used.

(ii) Current mailing address, including residential address if different than current mailing address.

(iii) Date and place of birth.

(iv) Social security number, (submission is voluntary, although recommended).

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

(vi) Alien registration number, if applicable.

(4) Must undergo a threat assessment by TSA prior to receiving authorization under this section and prior to boarding an aircraft operating into or out of DCA as provided in § 1562.23(d)(1) of this part.

(d) *Training.* Each armed security officer onboard an aircraft operating into or out of DCA must:

(1) Have basic law enforcement training acceptable to TSA; and

(2) Successfully complete a TSA-approved training course, developed in coordination with the Federal Air Marshal Service, at the expense of the armed security officer.

(e) *Armed security officer program.* (1) Each armed security officer onboard an aircraft operating into or out of DCA must—

(i) Comply with the Armed Security Officer Program.

(ii) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know, and refer all requests for SSI by other persons to TSA.

(2) TSA and the Federal Air Marshal Service may conduct random inspections of armed security officers to ensure compliance with the Armed Security Officer Program.

(f) *Authority to carry firearm.* An armed security officer approved under this section is authorized—

(1) To carry a firearm in accordance with the Armed Security Officer Program on an aircraft operating under a DASSP into or out of DCA; and

(2) To transport a firearm in accordance with the Armed Security Officer Program at any airport as needed to carry out duties under this subpart,

including for travel to and from flights conducted under this subpart.

(g) *Use of force.* Each armed security officer authorized to carry a firearm under this section may use force, including deadly force, in accordance with the Armed Security Officer Program.

(h) *Use of alcohol or intoxicating or hallucinatory drugs or substances.* An armed security officer onboard an aircraft operating into or out of DCA may not consume alcohol or use an intoxicating or hallucinatory drug or substance during the flight and within 8 hours before boarding the aircraft.

(i) *Credential.* (1) *TSA credential.* An armed security officer under this section must carry a credential issued by TSA.

(2) *Inspection of credential.* An armed security officer must present the TSA-issued credential for inspection when requested by an authorized representative of TSA, the Federal Aviation Administration, the Federal Air Marshal Service, the National Transportation Safety Board, any Federal, State, or local law enforcement officer, or any authorized aircraft operator representative.

(3) *Preflight identification to crewmembers.* When carrying a firearm, an armed security officer must identify himself or herself to all crewmembers either personally or through another member of the crew before the flight.

(j) *Suspension or withdrawal of authorization.* At the discretion of TSA, authorization under this subpart and 49 U.S.C. 44903(d) is suspended or withdrawn upon notification by TSA.

Issued in Arlington, Virginia, on July 15, 2005.

**Tom Blank,**

*Acting Deputy Administrator.*

[FR Doc. 05-14269 Filed 7-15-05; 3:06 pm]

**BILLING CODE 4910-62-P**