Privacy Impact Assessment
for the

AIRSPACE WAIVERS AND FLIGHT AUTHORIZATIONS FOR CERTAIN AVIATION OPERATIONS (INCLUDING DCA) (Amended)

September 20, 2005

Contact Point
Lisa S. Dean
Privacy Officer
Transportation Security Administration
(571) 227-3947

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

1. Overview

This Privacy Impact Assessment (PIA) is an updated and amended version of the PIA originally published on July 19, 2005. TSA has revised the information it intends to collect from Armed Security Officers (ASO) to include the collection of a photograph and electronic signature for use in preparing the ASO credential, as well as the collection of ASO weapon information. TSA has also developed a redress policy.

2. Program Overview

After the September 11, 2001 terrorist attacks, the Federal Aviation Administration (FAA) immediately curtailed all aircraft operations within the National Airspace System (NAS), except certain military, law enforcement, and emergency related aircraft operations. On September 13, 2001, the FAA took action to allow additional aircraft operations in some areas of the NAS. However, the FAA maintained flight restrictions over certain cities and sensitive sites. Although most specific temporary flight restrictions over particular cities or sites have been rescinded, some flight restrictions are occasionally reinstated in response to specific and general intelligence information regarding terrorist threats. These flight restrictions were issued via the U.S. Notice to Airmen (NOTAM) System. Further, while many aspects of the initial flight restrictions were cancelled, in the Washington, DC Metropolitan Area for Ronald Reagan National Airport (DCA), the FAA continues to impose several temporary flight restrictions at the request of the Departments of Homeland Security (DHS) and Defense (DoD) to assist them in their counter-terrorism mission. While operations of commercial aircraft operators with full TSA security programs have been permitted to resume at DCA, commercial operators that do not have full programs and general aviation operators largely have continued to be prohibited from operating into and out of DCA.

In order to fly into these restricted airspace areas certain aircraft operators must seek a waiver. The Transportation Security Administration (TSA) provides an analysis of the security aspects of requests for waivers, and established the Office of Airspace Waivers in October 2002 to manage this waiver process. A significant part of the waiver process consists of vetting individuals who will be on aircraft operated under a waiver into restricted airspace.

TSA shares responsibility for managing the waiver process with the FAA. The FAA manages the safety requirements for aircraft operators who apply to operate in restricted airspace, while TSA manages the security requirements. TSA collects the required information and conducts a security threat assessment. If TSA approves the waiver request, TSA forwards the request to FAA, and FAA reviews the request to ensure that it comports with applicable safety requirements. If FAA approves the waiver request, FAA issues the waiver, which TSA forwards to the requester. Both agencies work together to ensure safety and security of aircraft operations are met while seamlessly providing the freedom of flight and commerce within U.S. airspace.

In coordination with the FAA, the Office of Airspace Waivers currently issues several types of waivers, to include waivers for:

- Access for certain operations to Ronald Reagan Washington National Airport
- Access to the Washington, DC Flight Restricted Zone
- Major Sporting Events

- Disney Theme Parks
- Flight Training
- International Operations
- Special Events

In addition, TSA issues flight authorizations for certain operations into and out of DCA. TSA has reassessed the decision to prohibit flights into DCA of the smaller aircraft operated by commercial aircraft operators, and flights by general aviation aircraft. TSA has determined that the economic impact of closing DCA to these operations was unnecessarily severe, but that restrictions are nevertheless required as a matter of security. 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 authorizing these operations at DCA provided that aircraft operators comply with certain security procedures. These procedures are: Each aircraft operator and each fixed base operator that supports the operation must have appointed a security coordinator (see definitions below). For each flight into and out of DCA the aircraft operator must carry an armed security officer. Each security coordinator, armed security officer, flight crewmember, and all passengers must have been vetted by TSA by undergoing a security threat assessment. TSA has contemporaneously issued a rule, insert Title, setting out how an operator may obtain a flight authorization for such operations, which TSA issues in coordination with the FAA. 49 CFR part 1562 subpart B, 70 FR 41586 (July 19, 2005).

As part of these procedures and in support of vetting requirements, TSA collects personal information from each individual affected by these procedures.

The purpose of this Privacy Impact Assessment (PIA) is to provide details about this collection of information and how the airspace waiver and flight authorization programs impact the privacy of security coordinators, flight crewmembers, and passengers, including armed security officers, who apply for or are identified on an application for an airspace waiver or flight authorization to operate in restricted airspace, and the steps that TSA will take to minimize the burden on these aircraft operators and protect their information. The collection of information will differ slightly depending on the type of waiver/authorization requested and this PIA highlights the particular procedures for DCA flight authorizations throughout this document.

3. Definitions

Armed Security Officer- Security officers authorized to carry a firearm under 49 C.F.R. §1562.29.

DASSP- means the aircraft operator security program (DCA Access Standard Security Program) approved by TSA under 49 CFR part 1562 for aircraft operating into and out of DCA.

Fixed Base Operator- means an airport-based commercial enterprise that provides support services to aircraft operators, such as maintenance, overnight parking, fueling and deicing.

FBO Security Program – means the security program approved by TSA under 49 CFR part 1562 for FBOs to serve flights into or out of DCA.

Flight Crewmember- means a pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time. This does not include an armed security officer.

Gateway airport- means an airport that has been approved by TSA under 49 CFR part 1562 as a last point of departure for flights into DCA.

Passenger- means any person on an aircraft other than a flight crewmember.

Security Coordinator- the individual responsible for implementing the DASSP or FBO Security Program and other security requirements under 49 CFR part 1562.

4. System Overview

4.1 What information will be collected and used for this security threat assessment?

For airspace waivers, through aircraft operators, TSA collects and retains personal information that is used to conduct a security threat assessment on the flight crewmembers and passengers who will be onboard the aircraft while it is operating in restricted airspace. This information includes: (1) first name, (2) last name, (3) middle name (if applicable), (4) social security number (submission is voluntary, although recommended), (5) passport number (if applicable), (6) passport country of issuance (if applicable), (7) date of birth, and (8) place of birth. Although provision of one's social security number is voluntary, failure to provide a social security number may result in delays in processing the waiver application.

Special procedures apply for aircraft operators seeking flight authorizations for operations into or out of DCA. Under this program, aircraft operators and fixed base operators will be required to designate a security coordinator who is responsible for implementing the applicable security measures as outlined in the rule. TSA will collect fingerprints and the following information to conduct a fingerprint-based criminal history record check and a security threat assessment on the security coordinator: (1) first, middle, and last name, 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) social security number (submission is voluntary, although recommended); (5) citizenship status and date of naturalization (if applicable); and (6) alien registration number (if applicable). Although provision of one's social security number is voluntary, failure to provide a social security number may result in delays in processing the security threat assessment. TSA also will collect fingerprints and the information listed above from each flight crewmember and armed security officer who will be on board any aircraft operated under a flight authorization into or out of DCA. Finally, TSA will collect the information listed above, but not fingerprints, from each passenger who is not an armed security officer but who will be on board any affected aircraft operations into or out of DCA.

For individuals applying to serve as armed security officers onboard flights into and out of DCA, additional information will be collected including address, citizenship, personal history including employment, criminal, medical, education and training, experience including sworn law enforcement and military experience, and references. TSA will also collect and maintain a photo and electronic signature for use on the ASO credential and reissued credentials. The credential information may be provided to law enforcement authorities in the event of an incident. ASOs will also be required to provide the make,

model, caliber, and serial number of the weapon they intend to use in connection with the program. ASOs who are currently employed by a law enforcement agency must also provide a written authorization by their employing agency to participate as an ASO and specify whether an agency issued weapon is authorized for use. This information will be used to verify the individual's qualifications to perform the duties required of armed security officers onboard flights into and out of DCA.

4.2 Why is the information being collected and who is affected by the collection of this data?

The collection of this information is necessary in order to grant waivers and flight authorizations to aircraft operators who request to operate in restricted airspace. The collection of information from armed security officer applicants is necessary to determine which individuals are qualified to perform the duties required of armed security officers onboard flights into or out of DCA. Individuals including flight crewmembers, security coordinators and passengers, including armed security officers, who wish to enter into restricted airspace will be affected by the collection of information. The information that is collected will be used to conduct a security threat assessment on flight crewmembers, security coordinators, and passengers, including armed security officers, and may preclude participation in operations depending on the results of the security threat assessment.

4.3 What information technology system(s) will be used for this program and how will they be integrated?

For domestic airspace waiver requests, TSA uses the information submitted to check each flight crewmember and passenger against relevant databases maintained by the National Crime Information Center (NCIC). In addition to the NCIC check, information from flight crewmembers and passengers, including armed security officers, is checked against other Federal databases, including the Terrorist Screening Center Database (TSDB) and TSA Selectee lists. If a positive name match is found, the waiver request may be denied, or the particular flight crewmember or passenger may not be allowed on the aircraft.

For international airspace waiver requests, TSA uses the information submitted to check each flight crewmember and passenger against Federal databases, including the TSDB and TSA Selectee lists. If a positive name match is found, the waiver request may be denied, or the particular flight crewmember or passenger may not be allowed on the aircraft.

For requests to operate into or out of DCA under a flight authorization, TSA uses the information submitted to conduct a fingerprint-based Federal Bureau of Investigation (FBI) criminal history records check (CHRC) for each flight crewmember, security coordinator, and armed security officer. The CHRC is conducted at least one time, but may be repeated. In addition, TSA uses the information submitted to check each flight crewmember, security coordinator, and passenger, including armed security officer, against Federal databases, including the NCIC, TSDB and TSA Selectee lists to identify potential threats to aviation security. TSA checks flight crewmembers and passengers, including armed security officers, against Federal databases each time they fly into or out of DCA.

4.4 What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?

The application for an airspace waiver or flight authorization includes a Privacy Act statement as required by the Privacy Act of 1974 (5 U.S.C. 552a (e)(3)). The Privacy Act statement informs individuals of the reasons their personal information is being collected, the authority for the collection, and how their information will be used. The statement also informs individuals that the collection of information is voluntary, but that those who are not willing to provide the required information may not be eligible to board a flight that requires an airspace waiver or flight authorization.

4.5 Does this program create a new system of records under the Privacy Act?

No. The information collected for airspace waivers or flight authorizations, and from ASOs, is part of an existing TSA Privacy Act system of records known as the Transportation Security Threat Assessment System (DHS/TSA 002). The collection, maintenance, and disclosure of information are in compliance with the Privacy Act and the System of Records Notice for DHS/TSA 002.

4.6 What is the intended use of the information collected?

TSA will use the collected information to conduct a security threat assessment on individuals applying for approval as a security coordinator for an approved fixed base operator at a TSA approved gateway airport or for an aircraft operator authorized to receive flight authorizations into DCA, or as flight crewmembers or passengers, including armed security officers, onboard aircraft operating in restricted airspace pursuant to an airspace waiver or flight authorization. TSA will also use the information collected from ASOs to determine which individuals are qualified to perform the duties required of armed security officers onboard flights into or out of DCA.

The collected information will be maintained and stored for use by TSA when adjudicating subsequent requests for an airspace waiver or flight authorization. TSA will reevaluate each passenger and flight crewmember's personal information upon receipt of a new waiver or flight authorization application. TSA also will store and use the data for comparison to future application requests. A submitted name that results in a match to any of the databases used to conduct a security threat assessment will also be maintained. This information will be annotated for denied operations.

4.7 How will individuals be able to seek redress?

In the case of criminal history records checks (CHRC), if an applicant disputes the results of a CHRC (i.e., disposition of a charge (s) is incorrect), the applicant can provide court documentation to TSA's Office of Transportation Threat Assessment and Credentialing at the following address:

Transportation Security Administration
Attention: GA into DCA Program (TSA-19)
601 South 12th Street,
Arlington, VA 22202

If the applicant can show that the disposition(s) (or charge(s)) does not fall under the disqualifying offense category; he or she will be not be disqualified based on the offense(s). Similarly, if the applicant can show that corrected disposition or charge(s) no longer falls under the disqualifying offense category; he or she will be not be disqualified based on the offense(s).

Individuals who believe they have been incorrectly identified as a security threat will be given the opportunity to contact TSA's Office of Transportation Threat Assessment and Credentialing (at the address above) to address their concerns. Redress based on the security threat assessment will be handled on a case-by-case basis due to the classified and/or security sensitive information that may be involved. To the extent permitted by law, TSA will provide information on which the determination was based to the applicant. There may be items that are classified or sensitive security information that TSA cannot release. For the name based security threat assessment, TSA will be the final adjudicator for security threat assessments.

ASOs determined to be unqualified for reasons other than the security threat assessment (such as eligibility criteria or failure to pass training) may appeal that determination to the TSA Office of Law Enforcement.

4.8 With whom will the collected information be shared?

The personal information collected from security coordinators, flight crewmembers, and passengers, including armed security officers, will be shared with TSA staff and contractors on a need to know basis. It is also shared with the FAA. Once the FAA grants final approval of an airspace waiver, TSA electronically enters the aircraft operator's information (e.g., company name (if applicable), phone number, and address) into a Master Waiver List database. This database is distributed to FAA Air Traffic Control Towers. Any information collected also may be provided to governmental agencies when relevant for criminal and civil investigations concerning threats to civil aviation security or violations of law, rule, or regulations.

TSA will also maintain a list of qualified ASOs who expressly request to be on a list available to FBOs, aircraft operators, and security companies seeking qualified ASOs.

4.9 How will the information be secured against unauthorized use? (What technological mechanism will be used to ensure security against hackers or malicious intent?)

TSA will secure personal information against unauthorized use through a layered security approach involving procedural and information security safeguards. The data will be encrypted using National Institute of Science and Technology (NIST) and Federal Information Security Management Act (FISMA) standards and industry best practices when being transferred between secure workstations. Only TSA employees and contractors with proper security credentials and passwords will have access to this

information to conduct the security threat assessment. Moreover, all TSA and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data.

Specific privacy safeguards can be categorized by the following means:

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

The Privacy Act of 1974, as amended (5 U.S.C 552a), which requires Federal agencies to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of information protected by the Act.

Federal Information Security Management Act of 2002 (Pub. L. 107-347), which establishes minimum security practices for Federal security systems.

4.10 Will the information be retained and if so, for what period of time?

Information will be stored and retained until the National Archives and Records Administration (NARA) approves a record retention schedule for the information. Until such a schedule is approved by NARA, TSA is required to retain the information.

TSA will retain the applications and waiver/authorization approval letters indefinitely in locked file cabinets. The FAA also will securely store copies of the approval letters at FAA Headquarters indefinitely. The indefinite time period is necessary for retrieval, comparison, and solving data discrepancies in future waiver, flight authorization applications, and renewals.

4.11 What databases will the names be run against?

TSA will run names against Federal databases, including the NCIC, TSDB and TSA Selectee lists to identify potential threats to aviation security. These are national databases used by government agencies to determine and deter potential security threats and terrorist activity.

4.12 What is the step-by-step process of how the systems will work once the data has been collected for a flight?

The following step-by-step process is applied to each airspace waiver request TSA receives. TSA has highlighted differences in the DCA flight authorization process. TSA will process all the flight crewmembers and passengers identified on the application through the same security threat assessment. All personnel involved have been trained on the procedures for handling sensitive material. The following is the actual step-by-step process:

<u>Airspace Waiver</u>

- TSA receives an application and sorts according to flight date.

- A TSA program analyst reviews all information on the application to determine if the required information has been submitted.

- After the initial review of the application, the individual's information is checked against the TSDB and TSA Selectee list and submitted for an NCIC check.

- If all the flight crewmembers and passengers are cleared, TSA submits the application to FAA for final approval. If a flight crewmember or passenger is not cleared (i.e., name match to a person contained in one of the national databases), TSA informs the applicant that that individual is not approved to serve as a flight crewmember or passenger on the operation until further investigation has been completed.

- After the security threat assessment has been completed and cleared, the individual's personal information and date of approval are stored in a TSA database for future reference.

DCA Flight Authorization Process

To be eligible to apply for flight authorizations into or out of DCA, an aircraft operator first must adopt and implement a DCA Standard Security Program (DASSP). As part of the DASSP, the aircraft operator must designate a security coordinator, who must undergo a TSA security threat assessment, including a fingerprint-based CHRC. In addition, each flight crewmember who will operate on any aircraft into or out of DCA must undergo a TSA security threat assessment, including a fingerprint-based CHRC. Once the aircraft operator has complied with these requirements, the operator will be eligible to apply for flight authorizations to operate specific flights into or out of DCA. On each flight the aircraft operator will have to ensure that it has on board an armed security officer who meets the requirements of 49 CFR part 1562, which include that the officer has undergone a TSA security threat assessment that includes a fingerprint-based CHRC.

The following step-by-step process will be applied to each request for a flight authorization:

- TSA receives an application from an aircraft operator to operate a flight into or out of DCA.

- A TSA program analyst reviews all information on the application to determine if the required information has been submitted.

- After the initial review of the application, the individual's information is checked against TSA databases.

- The fingerprints are run against the NCIC to check for disqualifying criminal offenses, as set forth in 49 C.F.R. §1542.209.

- If all the flight crewmembers and passengers are cleared, TSA approves the application. If a flight crewmember or passenger is not cleared (i.e., name match to a person contained in one of the national databases) after the initial security threat assessment is conducted, TSA informs the applicant that that individual is not approved to serve as a flight crewmember or passenger on the operation until further investigation has been completed.

- After the security threat assessment has been completed and cleared, the applicant's name, social security number (if voluntarily provided), and date of approval are stored in a TSA database for future reference.

- Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?

All TSA personnel and contractors will be properly trained and evaluated on the process of issuing airspace waivers and flight authorizations, and processing armed security officer applications. This training will include how to correctly and efficiently handle sensitive as well as Privacy Act protected material. All staff members will also complete the TSA mandated privacy training.

In addition to the training, all TSA personnel and contractors must possess the appropriate credentials and clearances to access various databases, files, and other sensitive material. As described above, TSA will secure and lock all sensitive material at all times. Only trained and cleared personnel will be authorized the use of these documents.

FOR QUESTIONS OR COMMENTS, PLEASE CONTACT:

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 571-227-3813