UNITED STATES DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

Statement of

JOHN SAMMON
ASSISTANT ADMINISTRATOR
TRANSPORTATION SECTOR NETWORK MANAGEMENT

Before the

SUBCOMMITTEE ON TRANSPORTATION SECURITY
AND INFRASTRUCTURE PROTECTION
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

July 15, 2009

Good afternoon Chairwoman Jackson-Lee, Ranking Member Dent, and distinguished Members of the Subcommittee. It is my pleasure to appear today to discuss the security of general aviation (GA), a vital part of our Nation's aviation system, an important economic engine, and an essential link to larger communities for many small communities. As always, we appreciate the Subcommittee's support as we continue to explore optimal security measures for this industry.

The Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) are committed to ensuring that GA is appropriately protected from exploitation by terrorists and other security risks while ensuring the free flow of commerce. Following specific directions from Congress, we already have instituted a few targeted security measures tailored to the risk posed by certain GA operations. Our approach to the task of addressing GA security mirrors our approach to our overall mission of securing the Nation's transportation systems--we begin by assessing the risks and then we work closely with our stakeholders to fashion programs to address those risks.

General aviation encompasses diverse aircraft, airports, facilities, operators and operations. GA operators and their aircraft include recreational pilots, corporations that operate business jets for executive and employee use, and companies that lease small and large aircraft to individuals and corporations or manage aircraft on their behalf. Nationwide, there are more than 19,000 GA facilities (including helipads) at some of our largest commercial airports, at small exclusively GA airports in remote areas, and at airports of all sizes in between. Aircraft that are used in GA include, among others, small

aircraft with minimal payload capacity, business jets, and jets often used by commercial airlines, such as the Boeing 747.

Added to this structural diversity is a diversity of risk facing the industry. The level of risk does not necessarily correlate to the size or sophistication of a given aircraft or airport. As a result, general aviation presents unique challenges that preclude a "one size fits all" security program. Prevailing circumstances and risks--vulnerabilities, threats, and potential consequences--all factor into the formulation of our security approach. Accordingly, each of the elements of TSA's security agenda—whether initiated by TSA or specifically directed by Congress—has been or is being developed to address a specific risk associated with the GA system—its aircraft, airports, facilities, operators, and its operations.

DHS's Current General Aviation Security Rules and Programs

Currently, there is a range of security measures protecting GA operations. Some take the form of guidance that airports or airport operators may voluntarily implement, while other requirements are implemented pursuant to mandatory regulations and security directives. All are intended to meet the dual goals of protecting GA from terrorism and other security risks without unduly impacting the free flow of commerce. The following represent some of the major security initiatives.

Restricted Air Space Over the Nation's Capital. Soon after the 9/11 attacks, the Federal Aviation Administration (FAA) issued a rule defining the restricted airspace over the Washington, D.C. Metropolitan Area and established rules for all pilots operating aircraft to or from any of the three Maryland GA airports located closest to the National Capital Region (College Park Airport, Potomac Airfield and Hyde Executive Field, known as the "Maryland Three Airports"). This rule established regulatory requirements for operating aircraft within the defined areas, known as the Special Flight Rules Area and the Flight Restricted Zone.

Temporary Flight Restrictions (TFR). TFRs are employed to mitigate the threat of an airborne attack against key assets and critical infrastructure on the ground; they affect the general aviation community by prohibiting flight in areas of concern, for example, near sporting arenas for major events such as the Super Bowl. TSA evaluates requests for security-related TFRs based on several criteria, including specific and credible threat and intelligence information, the number of people in attendance at a particular venue, and the number of allocated defense assets. Additionally, the FAA-issued Notices to Airmen prohibiting many general aviation aircraft from operating within a specified distance above ground level of any stadium with a seating capacity of 30,000 or more people where major sporting events are being held, or of the Disney theme parks in California

and Florida, have been made permanent by Congress, pursuant to the Consolidated Appropriations Act, 2004, P.L. 108-199.

Additionally, the United States Secret Service in coordination with FAA, TSA, and the Department of Defense establish restricted airspace for specified Presidential and Vice Presidential movements, the United Nations General Assembly, as well as National Special Security Events such as the G-20 Summit and Democratic and Republican National Conventions.

DCA Access Standard Security Program (DASSP). Recognizing the need to normalize GA commerce while continuing to protect the National Capital Region, Congress directed DHS to develop a security plan to permit general aviation aircraft to resume operations into and out of Ronald Reagan Washington National Airport (DCA), where GA operations had been prohibited after 9/11. In coordination with other DHS agencies, the Department of Transportation, and the Department of Defense, TSA issued a rule, effective August 18, 2005, requiring TSA inspection of crews, passengers, property, and aircraft; TSA identification checks of passengers; submission of passenger and crew information 24 hours in advance of the flight; Security Threat Assessments (STAs) for all passengers; fingerprint-based criminal history records checks (CHRCs) for flight crew; and armed security officers on board each flight. On average, 20 flights per month into and out of DCA utilize this program.

Twelve-Five Standard Security Program (TFSSP). TSA currently requires aircraft operators that are air carriers or commercial operators with a maximum certificated take-off weight (MTOW) of more than 12,500 pounds (5,670 kg) to implement the TFSSP, which establishes mandatory vetting procedures of crew and passengers against the FBI Terrorist Screening Center's No Fly and Selectee Lists.

Private Charter Standard Security Program (PCSSP). The PCSSP is similar to the TFSSP, but for aircraft operators using aircraft with a MTOW of greater than 100,309.3 pounds (45,500 kg) or with a seating configuration of 61 or more, adds a requirement to physically screen passengers and their accessible property.

Maryland Three Airports. The Maryland Three Airports program was originally instituted by the FAA in order to reopen these airports, which, like DCA, had been closed to operations after the 9/11 attacks. The program was transferred to TSA in February 2005. In addition to defining the restricted airspace and establishing rules for all pilots using the Maryland Three airports (discussed above), the rule provides that in order to be approved to fly into or serve as a security coordinator for any of these airports an individual is required to submit certain information and successfully complete a STA.

General Aviation Airport Vulnerability Assessment Tool. Section 44901(k) of title 49, as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, requires TSA to develop and implement a standardized threat and vulnerability assessment program for GA airports, to evaluate the feasibility of a program to provide grants to GA airport operators to upgrade security, and to establish such a program, if feasible. The assessment tool contemplated by this provision is currently under review by the Office of Management and Budget. When released, this program will assist our stakeholders in performing self-assessments to determine their security needs. Their planners will be able to identify security needs and seek funding from appropriate sources.

Automatic Detection and Processing Terminal (ADAPT). The ADAPT system was developed by FAA to allow real-time vetting of air traffic operating in the National Airspace System (NAS) and neighboring airspace, in order to distinguish between legitimate flights and those that might pose a security risk to the United States. TSA identified the need to prevent the misuse of aircraft as weapons against critical infrastructure and to provide senior leadership with a common real-time picture of aviation activities in the NAS. TSA requires a single integrated solution that can incorporate all segments of aviation, with a primary focus on GA, and potential expansion to other modes of transportation.

ADAPT is particularly important to the GA community. By providing advance warning of potential threats within the NAS and allowing the monitoring of GA security anomalies before they arrive in the United States, ADAPT assists in mitigating two critical risks specific to GA: the use of GA aircraft as a kinetic weapon and the use of GA aircraft as a conveyance to transport dangerous materials (including chemical, biological, radiological, and nuclear weapons) or malevolent people.

Electronic Advance Passenger Information System (eAPIS). U.S. Customs and Border Protection (CBP) issued a final rule, effective May 2009, that requires more detailed information about GA aircraft arriving and departing the United States and persons onboard. As part of a comprehensive effort to strengthen GA security, the rule expands existing regulations governing these aircraft. Pilots must submit the following information one hour prior to departure for flights arriving into or departing from the United States: departure information; arrival information; information identifying the aircraft; and complete passenger and crew manifest data, identifying who is aboard the aircraft.

DHS Domestic Nuclear Detection Office (DNDO) and TSA. DNDO has led an effort to identify key vulnerabilities and threats associated with weapons of mass destruction, specifically with regard to radioactive and nuclear items. DNDO, together with CBP and

TSA, is working to facilitate international general aviation operations, while enhancing security for these operations and for the nation as a whole.

In April 2007, then-Secretary Chertoff directed CBP and DNDO to implement full radiological and nuclear scanning of all arriving international general aviation aircraft. DHS achieved this goal at the end of 2007. Today, all international general aviation aircraft are scanned upon arrival in the United States by CBP officers using handheld Radiation Isotope Identification Devices (RIIDs). Earlier last year, DNDO and CBP also conducted a testing program at Andrews Air Force Base to identify improved operating procedures using these handheld detectors and to determine requirements for improved next-generation technologies. These measures are part of a much larger initiative to create a Global Nuclear Detection Architecture to protect our country from radiological and nuclear threats whether they come by land, air, or sea.

Public, Consultative Process Is the Key to Effective Regulation

A critical aspect of TSA's regulatory approach is the process-oriented nature of devising mandatory security measures. DHS believes it is important to consult with stakeholders to better inform the department about the feasibility, benefits, and costs of these security options.

The Large Aircraft Security Program Proposed Rulemaking. As risk associated with air carriers and commercial operators has been reduced or mitigated, terrorists may view general aviation aircraft as more vulnerable and thus attractive targets. If hijacked and used as a missile, many of these aircraft would be capable of inflicting significant damage. In June 2006 TSA initiated a rulemaking process to address the risk associated with large GA aircraft. The Large Aircraft Security Program (LASP) demonstrates our ongoing commitment to government/stakeholder consultation. After engaging in outreach to the GA community, on October 30, 2008, TSA published a Notice of Proposed Rulemaking (NPRM) seeking comments on the proposed LASP. This NPRM marked the beginning of the process established by the Administrative Procedure Act for engaging the stakeholder community and the public at large in formulating new regulatory requirements.

TSA extended the formal comment period for the NPRM by 60 days from December 29, 2008, to February 27, 2009, to further facilitate industry input and encourage additional comments. During that time, TSA also conducted five public meetings throughout the country to solicit input from the GA community and other members of the public.

In the process of evaluating over 7,000 written comments received, TSA also actively engaged industry stakeholders and entities indirectly affected by the NPRM in comment sessions to discuss key issues of concerns raised during the formal comment period and

public meetings. These comment sessions have featured positive discussions focused on developing a security solution tailored to GA and have provided TSA with additional insight on potential alternative solutions that may be more feasible for industry to implement, while still maintaining an effective level of security.

TSA appreciates the participation of the many stakeholders who have contributed to this process, including the Aircraft Owners and Pilots Association (AOPA), the National Business Aviation Association (NBAA), the National Air Transportation Association (NATA), the General Aviation Manufacturers Association (GAMA), the Experimental Aircraft Association (EAA), the American Association of Airport Executives (AAAE), the National Association of State Aviation Officials (NASAO), the Airports Council International (ACI), and other valued stakeholders. TSA and DHS are now determining the path forward, based upon the feedback received from industry and the public. There will be additional opportunities for stakeholders and interested members of the public to review and comment on any modified proposal.

Security Directives (SD) 1542-04-08F and -08G. The productive interplay between TSA and the stakeholder community also is exemplified in the issuance and amendment of security directives (SD). Congress provided TSA authority to implement security measures without prior notice or opportunity for comment when deemed necessary to protect the transportation system. SDs are issued in response to emergent situations and may be amended to adjust requirements to evolving circumstances. The authority to issue SDs is not new--it had been exercised routinely by FAA for decades prior to the creation of TSA.

Whenever possible, TSA engages in a collaborative process with stakeholders when formulating these directives. The recent issuance of SDs relating to Security Threat Assessments and credentialing of individuals with unescorted access to secure areas of airports is illustrative. In the course of preparing the SDs, TSA consulted with key stakeholders, made changes in response to their feedback, and conducted several conference calls afterward to ensure they understood the contents of the revised directives. TSA also extended the deadlines to give airports significant time to comply.

The SDs, issued in December 2008 and June 2009, apply to federalized commercial airports with full TSA security programs in accordance with 49 CFR Part 1542. The SDs improve identification/work authorization verification procedures and expand biographic information collected for processing STAs to improve turn-around time and redress procedures. The SDs also establish minimum audit procedures for identification media and require identification media for unescorted access to areas of the airport for which identification was not previously required. Although the SDs do not apply directly to GA operations, they do affect GA pilots who use these regulated airports.

It is important to note that the need for these SDs followed several special emphasis inspections of airports across the country during which TSA found an unacceptable level of compliance with existing credentialing programs. Even with effective stakeholder outreach in the preparation of SD 1542-04-08-0F, some in the GA community later raised concerns about potential impacts on GA pilots. TSA responded to those concerns, on May 28, 2009, by issuing a revision, SD 1542-04-08G, that clarifies certain issues in SD-08F. The most significant for the GA community is a clarification that transient pilots need not obtain an ID at each airport they visit, only at their home airports.

The Inspector General's Report Validates Our Approach to GA Security

We are pleased that the DHS Inspector General's (IG) May 2009 assessment of TSA's role in GA security concluded that TSA's risk reduction regime has been appropriate. We do not disagree with the report's assessment of the level of threat to GA airports; we would emphasize that risk is composed of more than specific threats and it is our obligation to address the other risk components: vulnerability and consequence. We must address the risk associated with larger GA aircraft. We are gratified that the IG recognizes the effectiveness of our measured, collaborative approach toward further regulation of this industry. The IG's report reflected TSA's current efforts to promulgate new GA security regulations through the Large Aircraft Security Program rulemaking process.

Meeting the Challenges of Securing the GA System

While we have made progress in meeting the challenges of securing the GA system, we continue to consult with stakeholders to improve our efforts. Our goal remains clear: protecting GA from terrorist and other security risks while advancing the free flow of commerce. The GA security programs currently in place have diligently endeavored to meet those dual objectives. Our success is dependent in large part upon the collaborative relationships we maintain with stakeholders, which will continue as we consider new regulations.

Thank you, again, for the opportunity to address the security of this important sector of our aviation system. I will be happy to answer any questions you may have.