Aviation Modal Annex

Table of Contents
Aviation Modal Annex

1 Executive Summary

The comprehensive increase in measures to enhance aviation security following September 11, 2001, led to significant improvements in existing security processes, operations, and technologies in each area of the aviation transportation system. These efforts led to the current security posture of a multilayered, scalable, and flexible aviation security system that is responsive to varying threat levels as well as to the entire range of identified threats. This has effectively reduced vulnerabilities within the aviation transportation system. However, the ever-changing aviation threat environment continues to challenge the Federal Government and private industry to implement additional effective and efficient security measures.

As directed by the National Infrastructure Protection Plan (NIPP), the Transportation Sector-Specific Plan (TSSP) represents the combined planning contributions of the sector's security partners to develop a system wide approach to reducing the security risks within and across the transportation modes. The aviation mode's security partners include the Department of Homeland Security's (DHS) Transportation Security Administration (TSA), the Department of Transportation's (DOT) Federal Aviation Administration (FAA), airlines, the Department of Defense (DoD) airports, flight crews, air cargo industry members, State and local law enforcement, and passengers.

This Aviation Implementation Plan has developed in concert with the emerging National Strategy for Aviation Security (NSAS) and its supporting implementation plans, which are in the process of being finalized. The NSAS provides a broad framework that aligns the Federal Government's aviation security programs and initiatives into a comprehensive and cohesive national effort that will influence future aviation security activities. This TSSP Aviation Implementation Plan shares several common goals with the NSAS that purposely help to define an overarching framework for achieving the objectives of the NIPP. These common goals include calling on the Nation to use the full range of its assets and capabilities to prevent the Air Domain from being exploited by terrorist groups, hostile nation-states, and criminals to commit acts against the United States, its people, infrastructure, and other interests; ensuring the safe and efficient use of the Air Domain; and calling on the Nation to continue using the Air Domain for air travel and commerce.

The TSSP aviation modal vision is to achieve a secure, resilient and efficient network of airlines, other aviation operators, airports, personnel, and infrastructure to ensure the safe and efficient movement of people and cargo and to prevent exploitation of the aviation transportation system to carry out attacks. Supporting this vision are partnerships between government and private sector entities, and a threat-based, risk managed approach to enhance security measures that recognize the mode's diversity.

This Aviation Implementation Plan associates current programs within the aviation community with the Transportation Sector Security Goals and Key Objectives. The Plan also identifies approaches for determining the way forward in aviation system security. The NIPP risk management framework, which is used to identify and prioritize critical systems and assets, will support active program development. Risk mitigation options, including physical, process and institutional changes, will be considered for these systems and assets, and prioritized based on their alignment with transportation sector security goals, research and development strategic goals, and other guidance from sector stakeholders.

The comprehensive implementation of a risk management methodology for the aviation transportation system will result in a prioritized portfolio of risk mitigation activities that will be informed and updated based upon relevant risks to the mode. Through the partnership already established between government and industry, enhancements to the aviation security posture will be effected in consultation with all aviation security partners. Security shortfalls and subsequent funding deficiencies will be identified through this process. In addition, government aviation security resources will be leveraged in conjunction with those of industry to minimize cost and coordinate modal security enhancements.

With a view toward this end-state, the TSSP Base Plan and this Aviation Implementation Plan specifically focus on how the Transportation Sector will continue to enhance the security of its critical infrastructure and key resources. Programs to protect the aviation system are key to making the Nation safer, more secure, and more resilient in the face of terrorist attacks and other hazards.

It is with these goals and objectives in mind that the following plan is respectfully presented.

2 Overview of Mode

For aviation transportation system security purposes, the aviation mode comprises a broad spectrum of private and public sector elements. The mode's diversity and complexity require an integrated and flexible approach to security. The mode's core components are the National Airspace System (NAS), commercial airlines, charter operators, airports, general aviation, and air cargo.

Federal departments and agencies are responsible for establishing and enforcing regulations, policies, and procedures; providing criminal law enforcement; identifying potential threats and appropriate risk-managed countermeasures; defining and mitigating risks and vulnerabilities on the ground and in the air; providing overall guidance; and applying security measures to passengers, their carry-on items, flight crew, baggage, and cargo. Airlines, airports, flight crews, air cargo industry members, State and local law enforcement, and passengers also play key roles in the multilayered protective posture that has taken aviation security beyond where it stood on 9/11.

The Department of Homeland Security (DHS) TSA oversees aircraft operators, foreign air carriers, and airport security; provides criminal law enforcement; and cooperates with State and local governments, local airport authorities, and law enforcement agencies to ensure the security of aviation operations and facilities. The DOT, through the FAA, provides regulatory oversight for and operates the NAS, as the country's civil aviation authority and air navigation services provider. FAA, in cooperation with DHS and other partners, plans and implements diverse air traffic and airspace management-related measures to support national defense, homeland security, law enforcement, and national response efforts. In addition, FAA is responsible for securing manned and unmanned NAS facilities and systems. These entities, along with other government agencies and the private sector, have collaborated (see section 2.3) in preparing this Aviation Implementation Plan.

2.1 Vision of Mode

The aviation modal vision is to achieve a secure, resilient, and efficient network of airlines, other aviation operators, airports, personnel, and infrastructure to ensure the safe and efficient movement of people and cargo and to prevent exploitation of the aviation transportation system to carry out attacks, while protecting civil liberties of all individuals. This vision will be supported by partnerships between government and private sector entities and by a threat-based, risk managed approach to risk mitigation that recognizes the mode's diversity.

2.2 Description of Mode

The aviation mode is vitally important to U.S. prosperity and freedoms. Each day, commercial aviation moves millions of passengers and their bags through U.S. airports. In air cargo, U.S. air carriers flew 39.2 billion revenue ton miles, 16.1 billion domestic, and 23.1 billion internationally, in 2005.[1] Historically, General Aviation (GA) has accounted for more than 77 percent of all flights in the U.S., carrying more than 105 million passengers each year.[2] Combined, the various sectors of U.S. aviation provide for transporting passengers and goods vital to the continued health of the national economy.

[1] FAA Aerospace Forecast, Fiscal Years 2006 - 2017

[2] Aircraft Owners and Pilots Association Data Available at http://www.aopa.org/special/newsroom/stats/activity.html

The components of the aviation mode—the NAS, commercial airlines, commercial airports, GA, air cargo, and international programs—are discussed in more detail in the subsequent paragraphs.

National Airspace System (NAS). The NAS is the dynamic network of facilities, systems, regulatory oversight, services, airspace, and routes that supports flights within U.S. airspace, including that international airspace delegated to the U.S. for air navigation services. The DOT's FAA regulates and operates this service.

Commercial Airlines. Commercial airlines are regularly scheduled or public charter operations that are regulated under Title 49 of the Code of Federal Regulations (CFR). The regulations apply to both domestic and international operations flying within, from, to, or over-flying the United States. Although commercial operations typically use large transport category aircraft, any type of aircraft, from a piston single-engine aircraft to an intercontinental jet, may be used.

Air Cargo. Air Cargo is defined as property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. U.S. mail is not considered cargo and is covered under a separate security program.

Commercial airports are defined as airports with regularly scheduled commercial passenger service. Currently, there are approximately 450 commercial airports in the United States that utilize TSA screening resources. The network of civilian and civilian/military joint-use airports is clearly perceived to be an essential resource for the Nation's economic and psychological well-being. Airports are also symbolic of U.S. citizens' expectations of freedom of travel, and are increasingly becoming nodes at which many or all modes of transportation interface.

General Aviation. GA is defined as all segments of the aviation industry other than air carriers and military aviation. GA's 200,000 aircraft and 630,000 certificated pilots transport 145 million passengers each year and use some 19,000 landing facilities. The GA industry encompasses a wide range of activities, from pilot training to flying for business and personal reasons, charter operations, delivering emergency medical services, firefighting, law enforcement, and sightseeing. Operations range from short-distance flights in single-engine light aircraft to long-distance international flights in corporate or privately owned "wide-bodies" – and from emergency aero-medical helicopter operations (i.e., MEDEVAC) to airships hovering over open-air sporting events.

International Programs. The TSA International Programs Office is an integral but unique part of the intricate web protecting the U.S. civil aviation system. The International Programs Office protects international civil aviation at the point of origin en route to the United States or in select upstream locations, with the goal of ensuring freedom of civil aviation operations for people and commerce. The International Programs Office also provides global quality control for civil aviation security and assists in improving the international level of security through maintaining effective business processes for assessments, surveys, air carrier inspections, crisis response, and management, combined with dynamic strategic, tactical, and operational planning.

2.3 Government Coordinating Council (GCC) Sector Coordinating Council (SCC) Structure and Process

In late 2005, the Secretary of Homeland Security exercised his authority under section 871 of the Homeland Security Act to create a committee, not subject to the Federal Advisory Committee Act (FACA), to facilitate public-private consultation on matters of critical infrastructure protection. Under this umbrella authority, which the DHS Office of Infrastructure

Protection exercises, several committees have been formed to focus on protecting critical infrastructure in the Transportation Sector of the national economy. These include a Transportation Sector GCC (composed of agencies of all levels of government); a Transportation SCC (composed of representatives of the owners and operators of critical transportation infrastructure); and the Critical Infrastructure Protection Advisory Council (CIPAC), a forum in which the Transportation Sector GCC and the Transportation SCC consult with one another. The Aviation Government Coordinating Council (AGCC) and the Aviation Sector Coordinating Council (ASCC) have formed a Joint Aviation Plan Working Group (JAPWG) under the auspices of CIPAC. CIPAC acts as a partnership model for the transportation sector. CIPAC is responsible for facilitating and coordinating planning; implementing security programs; providing operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution from events both man-made and naturally occurring; and sharing information about threats, vulnerabilities, protective measures, best practices, and lessons learned. Representatives from the TSA and FAA JAPWG co-chair, have met weekly to review the TSSP and develop the Aviation Implementation Plan. Subject matter experts provided key input to the Aviation Implementation Plan, and the text was circulated to all JAPWG representatives for review, comment, and concurrence. In addition, mode-specific units of the Transportation Sector GCC and Transportation SCC have been established, including the AGCC and ASCC.

The membership of the ASCC includes representatives of owners and operators of critical aviation infrastructure. The ASCC acts to establish and implement the public-private partnership envisioned by the NIPP. In this effort, the ASCC facilitates outreach and coordination among its stakeholders to coordinate developing the Nation’s aviation security plans with the AGCC. Industry members of the ASCC include organizations such as the Air Transport Association, the Aircraft Owners and Pilots Association, the Boeing Company, the Cargo Airline Association, and the National Air Transportation Association.

Like the ASCC, the AGCC fosters communication across government as well as between government and private industry in support of the Nation’s homeland security mission. The permanent membership of the AGCC is comprised of senior executives or their designees from TSA, FAA, DHS Office of Infrastructure Protection, the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), and the National Association of State Airline Officials (designated state government official).

3 Implementation Plan

The three Transportation Sector Security Goals and supporting objectives described in the TSSP Base Plan apply broadly to the aviation mode. Risk-managed decision making is applied within the aviation mode to determine the actions (programs and processes) necessary to achieve the goals. Obtaining and achieving these goals rely heavily on a continued partnership between government and industry with a clear focus on implementing cost-effective, mitigating security measures that are both flexible and unpredictable.

3.1 Goals, Objectives, and Programs/Processes

The TSSP process for identifying sector security goals reflects the collaborative approach of the entire SSP development process, as directed by Homeland Security Presidential Directive (HSPD)-7. The Transportation Sector Security Goals presented in the Base Plan represent the consensus of the sector's security partners. To achieve long-term success in securing the aviation transportation system, the Transportation Sector Security Goals will need to be seamlessly integrated into a risk-managed decision-making framework. In the subsequent paragraphs, the Aviation Implementation Plan associates the Transportation Sector Security Goals and key objectives with specific programs within the aviation community. A number of regulatory, screening, law enforcement, military, and intelligence activities and programs are in place within the aviation community to attain these objectives. Appendix 1 to this plan lists the aviation programs and the Transportation Sector Security Goals they support.

3.1.1 Goal 1: Prevent and Deter Acts of Terrorism Using or Against the Transportation System

The objectives supporting Sector Goal 1 are:

- ❑ **Implement flexible, layered, and unpredictable security programs using risk management principles**

Increase vigilance of travelers and transportation workers

- ❑ **Enhance information and intelligence-sharing among transportation sector security partners**

As evidenced by the August 2006 plot against U.S.-bound flights from the United Kingdom, the large and dynamic aviation transportation system remains an attractive target for terrorists. Many security measures have been implemented or improved since the 9/11 terrorist attacks, and the Federal Government, in cooperation with its stakeholders, continues to work within the changing threat environment to identify and mitigate potential threats and risks to the aviation transportation system. Protecting critical infrastructure is a national and homeland security concern that continues to receive a high level of attention.

Because of these conditions and based on the presidential and congressional direction of the Aviation and Transportation Security Act (ATSA), TSA deploys approximately 40,000 highly trained Transportation Security Officers (TSO), who work at more than 700 security checkpoints and nearly 7,000 baggage screening areas each day. To ensure effective and efficient operations at airports, the TSO workforce must be well-trained and alert to the latest threats. TSOs follow established screening procedures for processing passengers and carry-on items through passenger screening checkpoints and for processing checked baggage through baggage screening checkpoints.

TSA, in cooperation with FAA, DOD, DOJ, and other key stakeholders, continues to strengthen aviation security to protect the U.S. from threats involving the aviation domain as outlined in the following paragraphs, using the Sector Goal Objectives as a framework.

Objective 1: Implement flexible, layered, and unpredictable security programs using risk management principles

To adapt to the ever-changing threat environment, a variety of steps may be taken to deal with recognized and unidentified risks. Aviation risks are generally based on two types of threats: the aircraft as a target for attack (e.g., hijacking, stand-off weapons, on-board improvised explosive devices) and the aircraft as a weapon (e.g., as seen on September 11, 2001, or as a delivery vehicle for a weapon of mass destruction).

Using risk management principles, a number of flexible, layered and unpredictable security programs have been implemented in the aviation domain. The aviation modal risk management approach incorporates the **Transportation Sector Systems-Based Risk Management (SBRM) methodology**. TSA's risk management program will account for systems-based, as well as asset-based, risks. The program will define the mode's risk profile; develop the standards and criteria for a common, relevant operational picture to aid stakeholders to make effective decisions; and generate a portfolio of alternative management strategies leaders can use to build action and investment agendas that improve the overall risk profile of the mode.

The following are examples of programs that meet Objective 1.

TSA deploys **Federal Air Marshals** (FAM) onboard U.S. carrier aircraft both internationally and domestically. With nearly 30,000 U.S. commercial flights each day, TSA employs a risk-based approach in selecting flights for coverage. This risk-based approach assesses risk as a function of consequence, vulnerability and threat/intelligence. The Federal Air Marshal Service (FAMS) Mission Operations Center, collocated with the Transportation Security Operations Center (TSOC), provides incident coordination and law enforcement support to FAMS on a 24/7 basis. FAMs are also assigned to all 56 FBI Field Office Joint Terrorism Task Forces (JTTF) and the National JTTF, where they are assigned cases based on relevance to the aviation/transportation domain. The FAMS coordinates foreign air marshal missions arriving in the United States, facilitates the logistics of these missions, conducts regular liaison with foreign air marshal programs, and conducts "train-the-trainer" programs for international air marshals.

By protecting the facilities that constitute the systems that in turn provide air traffic services, FAA ensures the operational availability of the NAS. FAA's **Facility Security Management Program** is a robust program for categorizing and assessing facilities and implementing protective measures. FAA security specialists assigned across the country conduct assessments and inspections at FAA facilities to determine compliance with facility security, communications security and classified information, public laws, national directives, and DOT policies that influence FAA security practices. This creates a security environment within FAA that reduces the risks posed by espionage, sabotage, theft, vandalism, terrorism, and other criminal acts.

Within the aviation mode, FAA is also responsible for investigating and enforcing **Hazardous Materials Regulations (HMR)** issued by the DOT Pipeline and Hazardous Materials Safety Administration. Most hazardous materials (HAZMAT) transported by air are in small non-bulk packages and are not subject to the HMR security plan requirements, which apply to persons accepting or offering bulk quantities (placarded amounts) of HAZMAT. Air carriers subject to TSA security program requirements are authorized to comply with any air-mode HAZMAT security plan requirements by following their TSA-approved security program. Separately, however, all persons involved in HAZMAT commerce must receive security awareness training in accordance with the HMR.

The FBI, through its **Airport Liaison Agent (ALA) Program** has FBI Special Agents assigned to each TSA regulated airport. FBI ALAs support and enhance efforts to prevent, disrupt, and defeat terrorism and criminal operations directed toward civil aviation. Additionally, the ALAs provide counterterrorism prepardedness, leadership and assistance to Federal, State, tribal, and local agencies responsible for civil aviation security.

Commercial airlines must comply with federal security regulations. The regulatory scheme can facilitate constructive government and industry communication when developing means and mitigation tactics for securing the aviation system. All domestic scheduled commercial airlines are required to follow a standard security program under 49 CFR 1544, depending on the type of operation. These programs are regularly amended to account for the changing threat environment, new technologies and practices, and measures no longer practical.

The complexity of the **air cargo** environment necessitates a deliberative risk analysis and consideration of available resources among a wide array of options. The rapid transport of goods by air to destinations throughout the Nation and the world is an essential service. Security measures that are integrated into air cargo operations can help minimize unnecessary delays. TSA seeks to strengthen shipper and supply chain security for vetting sources and integrity in transit; use advance information technology (IT) to identify elevated risk cargo through prescreening; identify, develop, and deploy technology and procedures for performing targeted cargo inspections; and inspect 100 percent of targeted cargo at a high level of system effectiveness.

TSA's air cargo security final rule codified security upgrades introduced since September 11, 2001, and requires additional security measures throughout the air cargo supply chain. The application of identification and access control requirements in all-cargo aircraft operations areas, screening of persons transported and service personnel who board all-cargo aircraft, and new standard security programs for operators of large all-cargo aircraft are required. TSA issued complete revisions of all aircraft operator and indirect air carrier (IAC) security programs to include comparable requirements for screening cargo and access controls to facilitate transfer of cargo without compromising security standards.

A number of key initiatives are underway to achieve these goals, including developing the **Freight Assessment System (FAS).** The FAS will screen all air cargo to identify elevated-risk shipments for aircraft operator inspection prior to flight. Data on shippers, agents, IACs, air carriers, consignees, contents of the shipment, and threat information will be incorporated into the risk assessment at a transactional level for domestic and international shipments. TSA is also developing and implementing enhancements to the **Indirect Air Carrier Management System** to process the approval of new and renewal applications for IAC security programs and to automate background checks of IAC officials and persons with unescorted access to cargo, as required by the new final rule.

Because of the size and diversity of the **General Aviation** industry, TSA uses a threat-based, risk management and consequence analysis approach to security. This means the agency will analyze credible threat intelligence information to determine and prioritize the risks, threats, and vulnerabilities that exist. Based on this approach, TSA has developed a layered security arrangement, which integrates the capabilities of TSA and the stakeholder community to increase security, using diverse and complementary measures rather than relying on a single point solution, to create programs and policies that are reasonable, feasible, and effective for industry, while maintaining an appropriate level of security. To complement the threat-based, risk-management and consequence analysis approach, TSA has established strong lines of communication and working partnerships with industry stakeholders to support, promote, implement, and develop security programs and policies.

While the majority of GA is unregulated for security purposes, TSA does regulate certain segments of the industry. Operators of large aircraft (above 12,500 pounds maximum takeoff weight) used in charter or all-cargo operations are mandated to comply with the security requirements set forth in one of the TSA-approved standard security programs. Additionally, TSA regulates certain flight activities in the National Capital Region (NCR), like the **Maryland Three Rule (MD-3)**, which focuses on three small Maryland airports in the Flight Restricted Zone, and the **Restoration of GA at Ronald Reagan National Airport (GA@DCA)**.

In accordance with TSA Security Directives (SD), international and domestic commercial aircrews who fly into, out of, and over the United States are required to submit those crews in a Master Crew List (MCL), and in Flight Crew Manifests (FCMs) for each applicable flight for vetting by TSA against terrorism-related watch lists. This function is accomplished between TSA's Office of Transportation Threat Assessment and Credentialing (TTAC).

TSA law enforcement personnel includes **Assistant Federal Security Directors** for law enforcement (AFSD-LE). The consolidated law enforcement presence provides prevention, protection, and response capabilities for TSA in the transportation domain. AFSD-LE's primary duties are to establish and maintain liaison with local, State, and Federal law enforcement authorities and to coordinate their activities within the transportation domain.

Deploying TSA **Visible Intermodal Protection and Response (VIPR) Teams** introduces an element of unpredictability to disrupt potential criminal or terrorist planning activities. These mobile teams, consisting of law and civil enforcement personnel, operate in aviation and other transportation systems to detect, deter, and defeat possible terrorist activity. TSA VIPR team deployments are designed to quickly and effectively raise the level of security in any mode of transportation anywhere in the country. The teams work with local security and law enforcement officials to supplement existing security resources and provide deterrent presence and detection capabilities.

The **TSA National Explosives Detection Canine Team Program** prepares and deploys hundreds of dogs to serve with State, regional and local airport law enforcement authorities. These mobile teams can quickly locate and identify dangerous materials that may present a threat to transportation systems and can be used in all areas of the airport environment. Explosives detection canine teams are used to search narrow and wide-body aircraft, vehicles, terminals, cargo warehouses, and luggage in the airport environment. TSA-certified explosives detection canine teams are required to dedicate a preset portion of their daily activities to screening cargo being tendered for transportation on passenger aircraft and surveillance of air cargo facilities and aircraft operating areas. A TSA-certified canine team must screen all priority mail parcels of a minimum specified weight and above that are transported on passenger aircraft.

Objective 2: Increase vigilance of travelers and transportation workers

A number of programs directly support the objective of increasing the vigilance of travelers and transportation workers. For example, FAA supports several programs including an ID media program for its personnel. It also conducts suitability investigations of employees and contractors; and carries out investigations of employees, non-employees, contractors, and airmen suspected of violating FAA orders and regulations. FAA provides investigative services for alleged criminal activity by airmen and other FAA certificate holders, use of unapproved aircraft parts, counterfeit certificates, falsification of official documents, NAS security violations, property theft, and alleged employee misconduct and criminal activity. In addition, all commercial drivers associated with aviation services seeking a HAZMAT endorsement must undergo a Security Threat Assessment conducted by TSA's Office of Transportation Threat Assessment and Credentialing (TTAC).

Many commercial airline security regulations increase transportation worker vigilance through mandated reporting requirements and employee security training. While this increases vigilance among a broad group of people, passengers must also be aware of suspicious activity. Further development of vigilance and outreach programs continues to enhance awareness.

Since intelligence identifies aviation as a focus of terrorists, whether as a target or for use as a weapon, many current initiatives focus specifically on high-risk passengers. Certain technologies, such as biometrics, have emerged to securely identify those passengers traveling aboard aircraft.

The **Registered Traveler** program has the potential to enhance security by biometrically identifying individuals who have completed favorable background checks, and may thereby expedite their screening process. This allows real-time screening to focus on other passengers using the aviation system who are not participating in the program. In addition to programs at the checkpoint, pre-screening enhancements continue to evolve to help identify passengers who pose the greatest risks to the aviation system. Also, the **Secure Flight** program is evaluating the transfer of the watch list vetting process from air carriers to the Federal Government in an effort to centralize vetting of all traveling passengers.

In the **air cargo** arena, IACs, and principal officials are being vetted through new automated systems, and background checks against Watch Lists are being conducted for all employees and contractors with unescorted access to air cargo. TSA's Known Shipper Management System collects and compares automated information against government and commercially available databases to validate shippers who are permitted to ship cargo aboard passenger aircraft.

TSA develops and makes available to flight and cabin crewmembers an advanced self-defense training program that includes appropriate and effective responses for defending against an attacker. In the **Crew Member Self Defense Training** (CMSDT) program, crew members receive and review a self-paced, interactive digital versatile disc (DVD) and student manual designed to familiarize them with basic self defense concepts and techniques, and then attend one day of hands-on training at a participating community college.

TSA also implements the **Alien Flight Student Program**, which conducts security threat assessments on foreign students seeking certain types of flight training and mandates security awareness training for all flight instructors.

Objective 3: Enhance information and intelligence-sharing among transportation sector security partners

While many security measures have been implemented or improved since the September 11, 2001, terrorist attacks, TSA continues to work, in cooperation with all government and industry stakeholders, to identify and mitigate potential threats and risks. Given the vast size and dynamic nature of the industry, it is necessary to evolve with the changing threat environment. The airline industry's flexibility and its partnership with the Federal Government can provide the means to implement essential security measures and thwart terrorist attacks both now and in the future.

Intelligence-sharing has made great progress since September 11, 2001, and this collaboration must continue. Intelligence-sharing both within government and abroad has been responsible for preventing attacks against aviation and other modes of transportation.

Every FAM is trained to report suspicious activities within the aviation domain. FAMs file Incident Reports for all suspicious activities that a FAM believes require an interview with the person(s) engaged in the activity, and Surveillance Detection Reports for activities that, in the FAM's professional judgment, do not require an interview but are suspicious in nature. Both of these raw reports, plus any suspicious incident reports submitted by airline employees and other individuals within the aviation domain are placed in the Tactical Information Sharing System (TISS) through a designated email address where they can be accessed and analyzed by FAMS and other law enforcement organizations. Airline employees are encouraged to send suspicious incident reports to the FAMS through a designated email address. These reports are also placed in the TISS database. In addition to TISS, there are a number of ongoing programs such as Screening of Passengers by Observation (SPOT) that are intended to identify suspicious activities within the aviation domain.

TSA firmly believes that while prioritizing vulnerabilities and threats is a vital component in securing the Nation's transportation sector, it is important to identify a broad spectrum of activities that could potentially be misused for terrorist purposes. Therefore, the agency continues to develop security guidance documents for GA airports, establish security protocols for corporate and fractional (group-owned) aircraft, and increase security awareness and vigilance using the **Airport Watch Program** and the **GA Secure Hotline**.

3.1.2 Goal 2: Enhance Resiliency of the U.S. Transportation System

The objectives supporting Sector Goal 2 are:

- ❑ **Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability**
- ❑ **Ensure the capacity for rapid and flexible response and recovery to all-hazards events**

To continue to improve the aviation transportation system's risk profile, TSA, FAA, and other Federal security partners will focus on activities that not only manage risk but also create resilience in the system, including activities focused on prevention and preparedness, as outlined below.

Objective 1: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability

A number of key programs support the management and reduction of risk associated with key nodes, links, and flows within the aviation transportation system to improve overall network survivability.

The capacity for rapid and flexible response and recovery is also provided by TSA's **Transportation Security Operations Center** (TSOC), a robust, fully operational operations center that is staffed 24/7 and comprised of three watches. One watch, the Command Duty Officer (CDO), enables TSOC to provide communication and coordination and to establish domain and situational awareness across the entire transportation infrastructure. A goal of the

TSOC is to create a robust information-sharing environment by educating the TSA community and forming partnerships that promote fluid information exchange.

TSA is the Executive Agent for the second TSOC watch, the National Capital Region Coordination Center (NCRCC). As such, it provides physical infrastructure and connectivity for other agencies, including North American Aerospace Defense Command, Northeast Air Defense Sector, FAA, FBI, U.S. Secret Service (USSS), U.S. Capitol Police, U.S. Customs and Border Protection, U.S. Coast Guard, and the Metropolitan Police Department (Washington, DC). The NCRCC provides air space security for the national capital region, coordinates the activities of the participating agencies, actively reconciles conflicting procedures, and integrates the roles of each NCRCC representative.

The third TSOC watch is the National Infrastructure Coordinating Center (NICC). A part of DHS's Infrastructure Protection division, the NICC maintains operational awareness of the nation's critical infrastructure and key resources. The NICC provides a mechanism and process for information sharing and coordination between government and industry partners.

FAA efforts are targeted at improving overall network survivability include establishing an interagency, real-time network called the **Domestic Events Network** (DEN), which enhances shared situational awareness and coordinated decision-making on real-time security incidents involving the NAS or otherwise affecting U.S. interests. The DEN is an unclassified telephonic conference among air traffic control facilities, military entities, government agencies, and law enforcement officials, allowing real-time information to be shared simultaneously among all entities responsible for analyzing and responding to significant aviation events. The **Command, Control, and Communications** (C3) program provides the engineering, implementation and maintenance support for FAA systems, which include the VHF/FM radio installations at nearly 900 locations nationwide and the fixed satellite installations at more than 100 airports and air traffic control facilities.

FAA also employs an integrated system of policy, procedures, personnel, facilities, and communications ensuring aviation officials have timely, accurate information to plan, direct, and control all aspects of FAA-essential operations and functions during emergency situations. FAA plans, directs, and manages its essential operations during emergencies through established emergency operations programs. These established programs include disaster management, pandemic influenza planning, C3, continuity of operations (COOP), and emergency-related exercises. FAA provides guidance and assistance to all lines of business, staff offices, and field elements.

FAA maintains continuous command, control and communications with its field elements, other government agencies, and the aviation industry to ensure aviation officials have immediate access to information. This is critical to managing events having an impact on the NAS, including natural disasters and Incidents of National Significance.

Finally, FAA designs and implements air traffic and airspace management-related security measures in concert with its partners, including air traffic control intervention, using Temporary Flight Restrictions (TFR) to protect sensitive targets, monitoring NAS operations, and participating in specialized security interagency mechanisms such as Man-Portable Air Defense System (MANPADS) Mitigation Plans.

Objective 2: Ensure the capacity for rapid and flexible response and recovery to all-hazards events

Ensuring that essential functions continue contributes to the resiliency of the transportation system. As a baseline of preparedness for the full range of potential emergencies, all Federal agencies are required to have in place a viable COOP capability, which ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. For example, in a catastrophic event, FAA support personnel would be deployed to a "best response" location. In a hurricane, for instance, personnel would be deployed to provide local communications support to responders. During an influenza pandemic, minimal support staff would be provided at critical locations and other support would be provided remotely. A terrorist event would likely result in full staffing of all specialties to support all affected locations for the duration of the event.

TSA's **Emergency Preparedness Division** (EPD) is also located at TSOC. EPD represents TSA in preparing, planning, and conducting exercises at all levels, from internal tabletop to national level multiagency events, simulating incidents requiring a response based on policies and procedures established for the entity involved. EPD also manages an After Action Report program to identify weaknesses and issues identified from exercises, assign offices to be responsible for correcting the reason for the problem, and track these assignments to ensure completion.

An ongoing TSA effort that will help ensure the capacity for rapid and flexible response and recovery to all-hazards events is the **Natural Disaster Preparedness Plan** (NDPP), currently under development. The NDPP will ensure continued aviation transportation system security and facilitate support for other Federal, state, and local emergency response operations in areas affected by disasters, while meeting the needs of TSA employees (e.g., allowing them to prepare their homes and evacuate their families). The NDPP facilitates planning, preparation, and resource allocation for Headquarters personnel, Federal Security Directors and staff, and disaster support teams that will respond to assist affected TSA operations. These response teams are trained, equipped, and exercised, making them ready to rapidly deploy in the event of a natural disaster.

3.1.3 Goal 3: Improve the Cost-Effective Use of Resources for Transportation Security

The objectives supporting Sector Goal 3 are:

- ❑ **Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria**

Ensure robust sector participation as a partner in developing and implementing public sector programs for Critical Infrastructure/Key Resource (CI/KR) protection

Improve coordination and risk-based prioritization of transportation sector security Research, Development, Test and Evaluation efforts

- ❑ **Align risk analysis methodologies with Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP**

Objective 1: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria

While the overall Transportation Sector SBRM methodology has been developed, specific implementation programs and tools are still evolving. The SBRM detailed in the TSSP contains a series of steps that must be completed to identify a comprehensive portfolio of mitigation options and countermeasures. Criteria for selecting the aviation mode's critical systems as well as the mode's critical assets must first be established to define the scope of risk management activities. These screening criteria will define what is "critical" within the mode. Once the systems and assets have been screened, the means to conduct vulnerability assessments, including physical, process, and institutional components, must also be defined. It is likely that a variety of tools and methodologies will need to be integrated to support the differences between systems and assets as well as differences between asset types. The resulting prioritized portfolio of risk mitigation activities will be informed and updated based upon relevant risks to the mode.

TSA monitors the flight activities of thousands of **Federal Flight Deck Officers** (FFDO) flying U.S. commercial passenger and cargo aircraft. Under the Arming Pilots Against Terrorism Act, TSA established a program to deputize eligible volunteer pilots of commercial passenger aircraft as Federal law enforcement officers to defend the flight decks of their aircraft with force, including deadly force, against acts of criminal violence and air piracy. The FFDO program was subsequently expanded to include pilots of all-cargo aircraft, flight engineers and navigators.

TSA's **Armed Security Officer** (ASO) Program enables eligible persons with sufficient law enforcement experience to provide armed security aboard GA aircraft authorized to operate into and out of Ronald Reagan Washington National Airport (DCA). TSA established security procedures that allow GA operations to resume at DCA, while protecting critical national assets from possible airborne terrorist attack. These procedures include a requirement that each GA flight operating into or out of DCA have onboard an ASO specially trained and authorized by TSA.

Each day hundreds of Federal Law Enforcement agents from the FBI, USSS, Drug Enforcement Administration and other organizations fly armed on domestic flights. Each day hundreds of armed Federal Law Enforcement agents fly on domestic flights. The **Force Multiplier Program** could allow the TSOC to track the movement of individuals from participating organizations, and provide situational awareness of law enforcement aboard an aircraft in the event of an incident.

Objective 2: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection

The aviation industry bears significant costs associated with implementing security measures. The Federal Government recognizes the need to integrate analysis of increased security measures with the safety and efficiency needs of the aviation transportation system. Given this, the government must constantly evaluate the burden placed on the industry while it addresses the current threat environment. Through the partnership already established between government and industry, changes to the security realm are almost always the result of consultation with aviation stakeholders. Through these discussions, government resources align with those in the industry to alleviate unnecessary costs and promote further security enhancements. It is critical that the Federal Government continues this ongoing partnership so future threats may be successfully mitigated while applying rational security developments. Working together in these partnerships will facilitate the systematic review of lessons learned so that cost effective but resilient security measures are implemented in the future.

Objective 3: Improve coordination and risk-based prioritization of transportation sector security Research, Development, Test and Evaluation efforts

Research and development (R&D) has always been essential to the Transportation Sector and represents a primary strategy to deter and prevent terrorist actions. Ongoing challenges to sector R&D efforts include the diversity of ownership of transportation sector assets, the inherent vulnerability of surface transportation, the constant evolution of transportation security, and the increasing dependency on intermodal and international transportation. For these reasons, continual involvement by the private sector and transportation sector stakeholders is paramount to successfully address these challenges.

TSA's risk assessment framework will be used to identify and prioritize critical systems and assets. Once the risks are identified, the areas of concern will be verified with appropriate government and stakeholder participants. Risk mitigation options, including physical, process and institutional changes, will be considered for these systems and assets. Assessing the options based on their alignment with transportation sector security goals, R&D strategic goals and other guidance from sector stakeholders will provide a prioritization of the mitigation options.

R&D requirements are derived using a "technology scan" approach of available options to be considered, including current best practices. From these requirements, development efforts are derived, often including identification of short-, medium- and long-term desired outcomes. If approved, the path results in either basic, applied, or development research program(s) or some combination thereof. These programs may then result in pilot test programs in appropriate labs followed by deployment or field-testing.

The Federal Government is introducing new pilot programs that integrate and coordinate various measures. For example, the great variety and composition of items to be inspected in air cargo pose a very different challenge from that of inspecting baggage. Pilot programs designed to identify innovative methods to protect the integrity of air cargo from the time of acceptance until tendering at the airport will evaluate tamper-evident and tamper-resistant seals and locks to secure air cargo in transit. To determine an optimal array of security measures, other programs will evaluate the effectiveness of canines to inspect a higher percentage of air cargo in various configurations as well as to determine the efficiency, effectiveness, and operational impact of other technologies. Personnel selection tools, cargo specific training programs, and training aids such as threat image projection that can superimpose stored images of threat objects in scanned images of cargo items are used to improve the human operator performance of the air cargo inspection system.

Since transportation sector R&D is a shared activity across the Federal Government and private sector, there is a great deal of insight to harness that will help in developing appropriate technology requirements. Many of these requirements will be addressed through normal planning and programming activities. If the capability does not currently exist, an examination of other programs will be conducted that may be adapted to address the need or direct new research and development activities through the grants process or other funding vehicles to encourage new design capabilities.

R&D inputs to requirements are also driven by the evolution of technology capabilities. The continual scanning for new technology advances across the government, private sector and academia enables greater potential deployment of technology-enabled solutions for enhanced security at the same or lesser cost than existing protection measures. It also reveals the potential for new security capabilities not previously considered.

Objective 4: Align risk analysis methodologies with RAMCAP criteria outlined in the NIPP

RAMCAP will be the primary tool used to assess risk at the asset level. RAMCAP process steps establish common criteria for conducting strategic risk analyses that can be applied across all 17 CI/KR sectors. Common criteria include using common terminology and reporting for defining Asset and Threat Characterization, Consequence and Vulnerability Analysis, Threat and Risk Assessment, and Risk Management. RAMCAP also provides a common, non-sector-specific reporting framework that can be used to normalize and compare assets from different sectors, enabling informed resource allocation and consequence mitigation decisions around the Nation's CI/KR.

DHS is currently using RAMCAP in the nuclear sector and piloting the tool in the chemical sector. Other sector module sets, such as transportation, will follow. The Transportation Sector will work with the appropriate organizational elements of DHS and the American Society of Mechanical Engineers to coordinate creating a RAMCAP version for the transportation sector. This effort will document guidance on approaches and methodologies for analyzing risks to assets associated with adversary attacks, identifying and developing countermeasures and consequence-mitigation strategies to reduce risks, and evaluating countermeasures and consequence-mitigation strategies using cost-benefit analyses and other methods to inform resource allocation decisions.

Once transportation modules have been created, RAMCAP results will allow the transportation sector to work directly with DHS and other Federal agencies to prioritize countermeasures for various assets from different sectors based on comparative risk analyses. This will in turn allow DHS and other agencies to implement security measures that employ the Nation's resources for maximum security. Until RAMCAP modules for the transportation sector are developed, facilitated assessments may rely more heavily on current transportation modules already defined and in use.

3.2 Effective Practices, Security Guidelines, Requirements, and Compliance and Assessment Processes

Although not a requirement for the Aviation Mode, this section is based on the Presidential Executive Order for Surface Transportation to identify and assist in developing Industry Effective Practices, Security Guidelines, Requirements, and Compliance and Assessment Processes. The initiatives outlined below represent a large body of Aviation Mode-specific plans that address the full range of aviation transportation system security issues, and are discussed in relation to their direct correlation to the goals and objectives previously mentioned in section 3.1. A listing of programs related to these plans can be found in appendix 1, which lists aviation programs organized by sector.

3.2.1 Industry Effective Practices

Industry effective practices are security measures or processes that private industry recognize (but the Federal Government does not formally recognize) as performance standards. They may cover a wide range of security areas, including risk assessments, employee screening, access controls, intrusion detection, IT security, awareness training, incident management, and exercises.

3.2.2 Security Guidelines

Security guidelines are any formal security-related guidance that the Secretary of Homeland Security recommends, for implementation on a voluntary basis, to enhance the security of a (surface) transportation system.

Common Strategy #2. TSA and FAA developed the current version of the Common Strategy in coordination with the FBI, the airlines, and other key stakeholders, following the 9/11 attacks to provide updated, consistent guidance to air crews on how to best handle a hijacking situation.

This guidance, which is integrated into TSA's Aircraft Operator Standard Security Program (AOSSP) and other programs addressing the user community, established a new strategy designed to deal with terrorist hijackers, who intend to cause mass casualties, in contrast with the conventional hijacker, whose motive might be ransom, escape from the law, political asylum, or publicity. Common Strategy # 2, which was originally implemented on January 18, 2002, addresses the use of plain language in controller-pilot communications; the critical need to defend the cockpit; and the use of special transponder codes. TSA, FAA, and their partners are continuing to refine and enhance the implementation of Common Strategy #2.

Recommended Security Guidelines for Airport Planning, Design and Construction. On June 15, 2006, TSA issued revised "Recommended Security Guidelines for Airport Planning, Design and Construction" to the commercial airport industry, providing security guidance on airport layout, security screening, emergency response, access control and communications, and other topics. This document is intended for professionals in the engineering, architecture, design and construction fields. A team composed of 10 government agencies and approximately 135 private sector experts in a wide variety of security, aviation and architectural disciplines worked 18 months to produce this document. All experts contributed their time and talent free of charge through the Airport Security Design Guidelines Working Group of TSA's Aviation Security Advisory Committee (ASAC). TSA continues to coordinate with the industry to update the guidelines periodically.

General Aviation Airport Security Guidelines/Information Publication (IP). In May 2004, DHS/TSA, in cooperation with the GA industry, developed an IP titled General Aviation Airport Security Guidelines. The IP acts as a set of best practices/guidelines and is a guidance document for individuals with oversight responsibility of GA airports and facilities. The IP offers recommended security measures that can be applied to GA airports regardless of size and type of operation, and will offer potential solutions to airports that presently want additional security enhancements. Furthermore, the IP is available on the DHS/TSA Web site; TSA encourages State, local, and county officials to use it to assess their respective GA airports.

Airport Watch/GA Secure. The main security focus for recreational flying has centered on enhancing security at GA airports where the bulk of these operations occur. TSA, in partnership with the Aircraft Owners and Pilots Association (AOPA), implemented the Airport Watch Program, which increases security vigilance with the flying public and directs industry to contact the GA Secure Hotline (operated by TSA/ TSOC to report suspicious activities. This program provides a mechanism for any GA pilot or airport employee to report suspicious activities to a central Federal Government focal point.

3.2.3 Security Requirements

Security requirements are regulatory actions, including security directives when necessary and appropriate, to implement measures to enhance the security of a transportation system.

Sensitive Security Information. 49 CFR Parts 15 and 1520, Protection of Sensitive Security Information, are regulations which regulate the release of various records and information including those obtained or developed during particular security activities.

Security Regulations/Programs. For commercial aviation, 49 CFR 1544 describes all required security measures for aircraft operators and outlines the various security programs that particular aircraft operators must use, depending on its operation. Six unique programs are outlined in section 1544: the full, private charter, twelve-five, partial, all-cargo and limited programs. Unlike the passenger and baggage screening procedures performed by TSA, these measures generally do not take place within public view and are almost always performed by aircraft operators. Some of the procedures each carrier is responsible for performing—depending on the program—include vetting passengers against TSA No-Fly and Selectee Lists, searching the interior and exterior of aircraft, screening and securing cargo, and developing a security training program for crewmembers.

Airport Security Program (ASP). 49 CFR Part 1542 provides baseline security requirements for defined types of commercial airports. Under the regulation, airport operators must adopt and comply with an Airport Security Program. Once the airport operator develops the ASP, the Federal Security Director (FSD) must review and approve it. When approved, the ASP becomes the vehicle by which TSA can inspect and enforce security measures. An authorized Airport Security Coordinator (ASC) has custodial responsibility for the ASP and must inform TSA of any proposed changes to it.

Security Directives (SD) and Emergency Amendments (EA). Because of the ever-changing risks to commercial aviation, government and industry stakeholders, IACs, and foreign carriers must proactively develop new procedures to mitigate threats or address security loopholes. Based on specific intelligence information or other appropriate circumstances the government issues SDs/EAs to make rapid security adjustments. SDs/EAs require aircraft and airport operators to implement new security procedures, often on short notice. SDs are developed to mitigate certain threats, provide security measures for travel to specified airports, and develop adjusted procedures for changes in the Homeland Security threat level.

Security Advisory. On a continuous basis, TSA uses a threat-based, risk management, and consequence-based approach, including analyzing intelligence information, to monitor the security environment surrounding commercial aviation operations and assets, as well as those of GA. TSA will develop and disseminate a Security Advisory in the event a situation arises that requires increased scrutiny and vigilance among the American public. These advisories are given wide spread dissemination through the cooperation of aviation industry associations and Federal, State and local authorities. A Security Advisory is a summary of relevant and timely facts on GA security that is meant to increase security awareness.

MVA/MMP. TSA, in cooperation with the FBI, FAA, airport operators, local law enforcement, and other key stakeholders, has conducted MANPADS Vulnerability Assessments (MVA) at over 300 airports around the country. These MVAs have been used to establish airport-specific MANPADS Mitigation Plans (MMP), which the local FSD, in consultation with the aforementioned partners, exercises, updates, and manages. In accordance with national-level MANPADS guidance, the MMPs establish roles and responsibilities of the various stakeholders; notification procedures; countermeasures (e.g., strategic deployment of law enforcement assets to probable launch areas); and crisis response processes. TSA, FAA, FBI, and their other partners are continuing to refine and strengthen these MMPs.

Twelve Five Standard Security Program (TFSSP). This program provides security requirements for charter operators in aircraft with a maximum takeoff weight more than 12,500 pounds operating under under 14 CFR Part 135. For example, the program requires that pilots be vetted through the TSA security program and passengers be checked against the No-Fly List.

Restoration of GA at Ronald Reagan National Airport (GA@DCA). This program permits the reutilization of DCA by certain GA aircraft that apply for and comply with the regulation and program. The program requires that crewmembers be vetted; passengers be checked against the No-Fly List; an armed security officer fly with passengers into/out of DCA; all crewmembers and passengers and carry-on baggage be screened; and TSA inspect the aircraft prior to departure. Additionally, the rule requires fixed-base operators (FBO) to comply with the FBO standard security program.

Maryland Three Rule. This program authorizes the operation of three Maryland GA airports within the DCA flight restricted zone (FRZ). Airports must comply with the MD-3 security program and pilots must be vetted by TSA and FAA and be issued a personal identification number to be permitted to file a flight plan into the FRZ.

3.2.4 Compliance and Assessment Processes

Compliance and assessment processes are methods used to measure compliance against effective practices, security guidelines, or security requirements. Compliance and assessment processes can take the form of regulatory inspection, voluntary inspections, risk assessments, data calls, or other methods.

Compliance and Assessments. The TSA Office of Compliance is responsible for enforcing aviation security regulations and programs. TSA employs hundreds of Aviation Security Inspectors (ASI), at airports across the United States, to conduct compliance inspections of air carriers and work with regulated entities to help correct identified security deficiencies. Each aircraft operator is also assigned a Principal Security Inspector (PSI) to ensure overall security compliance at the corporate level. TSA deploys aviation security personnel to assess foreign airports, from which U.S. and foreign air carriers operate to the United States, for compliance with the security standards of the International Convention on Civil Aviation (Chicago Convention). If the Secretary of DHS finds, based on TSA’s assessment, that an airport has failed to implement appropriate security measures, the Secretary notifies the foreign government authorities of that decision and recommends steps to achieve compliance. If the airport fails to comply within 90 days of such notice, DHS must publish a notice in the Federal Register that the airport is noncompliant, post its identity prominently at major U.S. airports, and notify the news media. In addition, U.S. and foreign air carriers providing transportation to the airport from the United States must provide written notice to passengers of the decision on or with the ticket sold for flights to that airport. The Secretary may also “withhold, revoke, or prescribe conditions on the operating authority” of an airline that flies to that airport, and the President may prohibit an airline from flying to or from said airport from a point in the United States

In addition, TSA inspects foreign air carrier stations from which flights operate to the United States, as well as all U.S. air carrier stations located overseas. TSA deploys inspectors to specified foreign locations when the threat level indicates the need for their presence. Principal Security Inspectors (PSI) are assigned to liase with foreign air carriers and all-cargo aircraft operators. The PSIs are part of TSA’s International Programs’ Foreign Air Carrier Security Program. Under the Foreign Airport Assessment Program and Air Carrier Inspection Program, International Programs assesses more than 300 Category A and B international airports, inspects more than 454 U.S. carrier stations overseas, and inspects more than 294 foreign air carrier stations with operations to the United States.

The International Programs Office is responsible for liaison with foreign air carriers under the Foreign Air Carrier Security Program. Some 150 foreign air carriers and 30 cargo carriers have security programs with operations into the United States. In fiscal year (FY) 2004, International Programs conducted more than 550 air carrier inspections of foreign and US air carriers at foreign airports. Legislation for this program will require that all FAA-certificated Part 145 repair stations be subject to security regulations. It will further require all foreign repair stations to undergo a security review and audit. TSA is developing the Foreign Repair Station Program to ensure the security of maintenance and repair work conducted on US air carrier aircraft and components at domestic and foreign repair stations, as required in 49 U.S.C. 44924.

Crew Vetting Program (CVP). TSA's Office of Transportation Threat Assessment and Credentialing (TTAC) administers the CVP which vets foreign and domestic aircrews flying internationally into, out of, and over the United States against terrorism watch lists.

Alien Flight Student Program (AFSP). The AFSP requires foreign flight students who plan to participate in certain types of flight training submit information for a security threat assessment before commencing that training. The rule and program also require flight training providers to register with TSA and participate in security awareness training. Additionally, the program enables TSA inspectors to inspect all flight training providers.

Facility Security Management Program (FSMP). The FAA FSMP establishes security requirements for all FAA facilities and standard procedures for facility security management, control, and safeguarding personnel facilities. FAA security specialists conduct assessments and inspections to determine compliance with facility security, communications, security, classified information, national directives, and DOT policies that influence FAA security practices.

3.3 Grant Programs

DHS has several security grant programs and TSA provides technical assistance in evaluating grant proposals. TSA also provides technical evaluations during the processing of FAA AIP grants. The FAA's AIP provides grants to public agencies—and, in some cases, to private owners and entities—for planning and developing public-use airports that are included in the National Plan of Integrated Airport Systems (NPIAS). NPIAS identifies public-use airports that are important to public transportation and contribute to the needs of civil aviation, national defense, and the U.S. Postal Service. Eligible projects include those improvements related to enhancing airport safety, capacity, security, and environmental concerns. In general, sponsors can use AIP funds on most airfield capital improvements or repairs except those for terminals, hangars, and non-aviation development.

Risk assessment for AIP funding occurs on both the national and local level. Because the demand for AIP funds exceeds the availability, the FAA bases distribution of these funds on present national priorities and objectives. AIP funds are typically first apportioned into major entitlement categories such as primary, cargo, and general aviation. Remaining funds are distributed to a discretionary fund. On the local level, independent risk assessment studies are conducted at airports requesting AIP funds, with their nature relating directly to the needs of the particular airport. The AIP process does not include an internal risk assessment study, rather external studies are referenced to determine priorities and objectives on the national level as well as to define eligible projects for individual facilities.

Safety and security projects are two interwoven development categories under NPIAS. They include development that Federal regulation, airport certification procedures or design standards require, and are intended primarily to protect human life. These two categories, which combined account for five percent of the funding needs identified in the NPIAS, include obstruction lighting and removal, fire and rescue equipment, fencing and security devices. Safety development totals an increase of 23 percent from 2001 to 2005, while security costs total an increase of 69 percent in the same period. This increase reflects the costs associated with improving runway safety areas as well as the costs associated with modifying terminals to accommodate explosive detection systems and other security enhancements. FAA gives safety and security development the highest priority to ensure rapid implementation and to achieve the highest possible level of safety and security. AIP funds are drawn from the Airport and Airway Trust fund, which is supported by user fees, fuel taxes, and other similar revenue sources.

3.4 Way Forward

The Federal Government responded to the attacks of September 11, 2001, with a comprehensive increase in measures to enhance aviation security. Significant improvements were made to existing security methodologies, operations, and technologies through creating systems of security in each area of the Aviation Transportation System. The Federal Government established a scalable, flexible aviation security system that is responsive to varying threat levels and to the range of current and future threats to the U.S. and effectively reduced vulnerabilities within the Aviation Transportation System. Significant enhancements were made in the ability to detect threat objects and explosives that could be brought on or otherwise used against aircraft, and increases in the security posture of the entire Air Domain were made.

Collectively, these security measures have created multiple barriers, greatly reducing the likelihood of a successful attack. These measures represent important steps forward, but no individual component is totally fail-safe. Moreover, terrorists are continuing to devise methods for defeating security efforts, as evidenced by the recent threats to U.S.-bound flights the United Kingdom identified.

The ever-changing threat environment in the aviation transportation system provides numerous challenges to the Federal Government and private industry for implementing effective and efficient security measures. To continue addressing the persistent threat, government and its aviation stakeholders must cooperate in developing a layered security system through established programs and innovative enhancements.

Public-private engagement will be a key component in securing cyberspace. TSA will work with private and public-sector members within the aviation industry to promote and enhance cyber-security. TSA will also function as a resource to the aviation community by providing consulting and assistance in the following areas:

- **Assessing cyber risk periodically**
- **Developing policies and procedures that are based on risk assessments**
- **Developing subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate**
- **Providing security awareness training**
- **Testing and evaluating the effectiveness of information security policies, procedures, practices, and security controls periodically;**
- **Developing a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency**
- **Outlining procedures for detecting, reporting, and responding to security incidents**

- ❑ **Developing plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the aviation industry**

Looking forward, the Federal Government, in coordination with its industry partners, will evaluate the need to amend aviation security programs to address potential vulnerabilities and gaps. In addition, employee security training programs will continue to evolve for the increased protection of passengers and aircraft, with a special emphasis on vigilance and suspicious activity detection.

The Federal Government, in coordination with stakeholders, will continue to communicate security changes and threat information to educate the traveling public. Improved intelligence will assist with these efforts as information-sharing increases among all Federal agencies. Intelligence-sharing must continue to be enhanced to ensure threats to the aviation system are constantly in focus. It is critical that aviation stakeholders remain educated and flexible to adapt to any changes in security procedures and to ensure that new procedures are instituted quickly and accurately. Likewise, the Federal Government must continue to be proactive but prudent to ensure that any strengthened measures do not place unnecessary burdens on the industry.

Looking to the future, several government initiatives intersect around aviation security. In particular, two organizations are joining forces to plot the way forward to the airport of the future, in which security measures will result in minimal adverse operational impacts, while focusing scarce resources on vulnerabilities identified through a risk-vulnerability-consequence review. These organizations are the Security Identification Display Area (SIDA), SIDA II Work Group (SIDA II) within TSA, and the Security Integrated Product Team (SIPT) of the Joint Planning and Development Office (JPDO).

The mission of SIDA II is to review and, where necessary, redesign the current state of those security requirements applied in separating of the public (land side) from the nonpublic (airside) portions of airports. Under SIDA II, the main areas currently under review are Background Checks and Access Authority, Perimeter Access Controls, and Airside Response and Surveillance.

The JPDO was established in 2003. Its mission is to transform the U.S. aviation landscape from the current state to that of 2025 and beyond. The vision is to accommodate an anticipated three-fold increase in demand, while ensuring a superior level of safety, efficiency and security that has been the hallmark of the American aviation system. With focus on safety, security, the environment, and international cooperation, the JPDO will work cooperatively with SIDA II to leverage resources and shared visions to design and implement the security infrastructure that will ensure a robust and secure aviation environment.

FAA's Next Generation Air Transportation System (NextGen or NGATS) initiative is a complete air traffic system redesign to enable FAA to reduce delays, improve aircraft management, and maximize safety and efficiency. FAA is working with the National Aeronautics and Space Administration, DHS, DOD, and the Department of Commerce to expand the NGATS initiative beyond capacity to include security and national defense. The U.S. Air Force and FAA are working together, for example, on how to accommodate the growing numbers of unmanned aerial systems. FAA has included several stakeholders in this initiative, to include State and local governments, the Aerospace States Association, made up of lieutenant governors and governor-appointed delegates, and private sector stakeholders.

Numerous government and industry studies have identified potential areas of improvement in the security of the air cargo system. TSA and its partners are forming a number of initiatives they believe will meet future challenges in assuring air cargo security. Long-term improvement efforts have been implemented, including developing comprehensive cargo-security programs and incentive-based programs. Some of these programs can be found in appendix 1 of this document.

The sheer volume of air cargo combined with current technology limitations makes inspecting all air cargo challenging. The flow of commerce is similar to an airline hub-and-spoke system, with thousands of input lines feeding in to a relative few number of system access points. The combination of diversity of ownership and decentralization of access control associated with this supply system creates a unique challenge to anticipate, coordinate, and plan for air cargo security concerns from origin to destination. This curb-to-cargo-hold challenge will be a focus area of future R&D programs.

Because of the wide variety and scope of GA aircraft and landing locations, any approach to implementing security guidelines must consider the various types of flight operations as well as the size of aircraft involved, among other factors. Therefore, a flexible, common-sense approach to GA airport security is important if the industry is to retain its economic vitality.

For GA, TSA will continue to use a threat-based, risk management, and consequence analysis approach to analyzing and prioritizing the vulnerabilities and threats to GA assets and conveyances. This approach includes the continuous review of existing security programs and policies to align security measures with vulnerabilities and threats, to reduce security loopholes, and to implement reasonable/feasible security requirements that maintain an appropriate level of security. As intelligence information and vulnerabilities in the GA system are identified, TSA will modify existing and develop new programs and policies to address the threat.

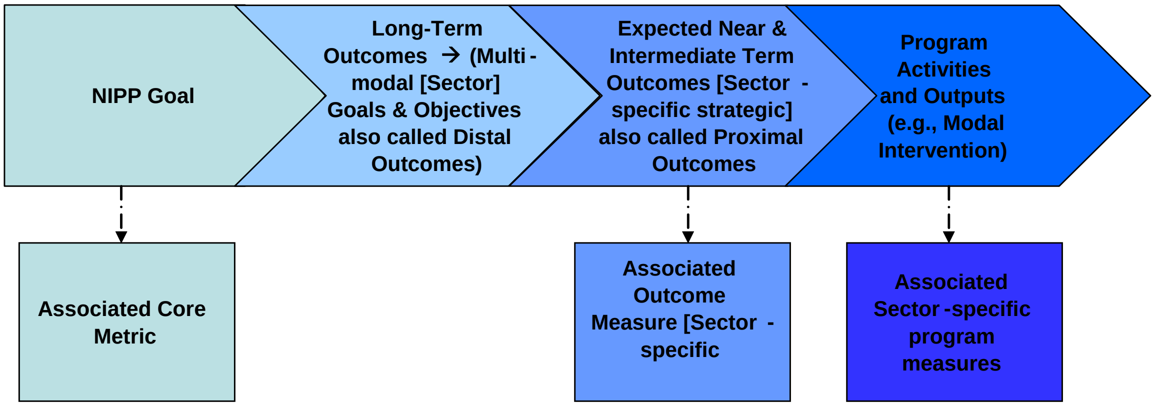
3.5 Metrics

General. To evaluate the collective impact of the transportation sector's efforts to mitigate risks to the transportation infrastructure and to increase the resilience of the transportation system through information-sharing mechanisms, measures of effectiveness must be developed and monitored. Metrics that are developed will supply the data either to affirm that TSSP goals are being met or to show what corrective actions may be required. This section overviews the plan to implement a TSSP measurement program. To be effective, the measurement program will require the cooperation of all modal GCCs and SCCs to provide accurate responses to the metrics being used to measure sector risk posture, TSSP effectiveness in the sector, and security program effectiveness.

Measurement Joint Working Group. A Measurement Joint Working Group will be formed under the Transportation Sector GCC/Transportation SCC and will be comprised of one member from each modal GCC and SCC or their designate and invited measurement professionals. Under the leadership of TSA's lead measurement organization, the group will operationalize measures; establish data sources, data collection and verification procedures; set measurement policy for the TSSP; and approve supporting procedures. The group may also require standardization of certain measurement practices from data contributors across the sector. The Measurement Joint Working Group will communicate regularly with Transportation Sector GCC/Transportation SCC members to ensure that working group progress and plans are fully transparent and coordinated with the members. In addition, work products of the Measurement Joint Working Group will be submitted, when appropriate, to the overarching Transportation Sector GCC/Transportation SCC for approval.

Measures. The Outcome Monitoring methodology as exemplified in figure 3-1 demonstrates working down from the national and multi-modal (sector) goals to determine outcomes and their respective measures.

Figure 3-1: Outcome Model


NIPP Goal
Long-Term Outcomes → (Multi-modal [Sector] Goals & Objectives also called Distal Outcomes)
Expected Near & Intermediate Term Outcomes [Sector - specific strategic] also called Proximal Outcomes
Program Activities and Outputs (e.g., Modal Intervention)
Associated Core Metric
Associated Outcome Measure [Sector - specific
Associated Sector-specific program measures

As discussed in chapter 6 of the TSSP Base Plan, the Transportation Sector's metrics have been segmented into two categories, which are:

1. Core: As discussed in chapter 6 of the TSSP, core NIPP metrics are common across all sectors and focus on measuring risk reduction progress in the sector. These measures are often descriptive statistics (counts).
2. Sector-specific: These metrics are used to gauge the overall effectiveness of the sector toward meeting TSSP goals and objectives. Ordinarily, these are outcome measures capable of quantifying the degree to which the SSP is "affecting" sector security. However, output measures are currently serving as proxies for the long-term outcome measures.

4 Program Management

The TSSP Base Plan presents an approach for the aviation mode to capture, comprehend, and explain the relationship between setting priorities ("What are we concerned about?"), developing programs ("What are we going to do about it?"), and understanding current capabilities ("What are we doing now?") to set a clear direction for risk management efforts. The goal of this approach is a scalable and agile multi-stakeholder security system that makes the most of scarce resources to protect the Nation's critical aviation transportation system infrastructure in a complex and constantly evolving environment.

The TSSP Base Plan points out that Planning, or gaining an understanding of how business is being done today in the aviation mode (the "as is" state), is a key first step to determining where the mode needs to be in the future (the "to be" state). The second step is Programming, or implementing an effective balance of programs while avoiding unnecessary duplication of effort and also preventing dangerous gaps. Finally, in the Budgeting phase, lead Federal partners will provide detailed budget justifications and program execution plans.

As noted in the Base Plan, maintenance of security programs—and their continued contribution to the sector's resilience strategy—is a shared responsibility. The Federal partner is responsible for the planning, programming, and budgeting steps, and will maintain federally operated programs. The Federal partner will also be responsible for providing standardized feedback and conducting an annual survey on the effectiveness and efficiency of its programs. This feedback will be used to guide program sustainment or adjustment and to collect best practices and lessons learned in developing new programs.

The success of any aviation transportation system security program is based in large part on the input and cooperation of relevant stakeholders. Coordination and communication with stakeholders is vital to ensure that any changes in Federal program execution (including termination) that will impact other programs or planning efforts at any level are properly explained and efficiently carried out.

As described earlier in this Annex (section 2.3), the Secretary of Homeland Security exercised his authority to create a committee to facilitate public-private consultation on matters of critical infrastructure protection. Under this umbrella authority, several committees have been formed to focus on protecting critical infrastructure in the Transportation Sector of the national economy, including the Transportation Sector GCC.

The Transportation Sector GCC is composed of agencies of all levels of government: a Transportation SCC, composed of representatives of the owners and operators of critical transportation infrastructure; and the CIPAC, a forum in which the GCC and SCC consult with one another. In addition, mode-specific units of the Transportation Sector GCC and Transportation SCC, like the AGCC and the ASCC, have been established.

The AGCC and the ASCC have established a JAPWG, under the auspices of the CIPAC, to assist with writing the Aviation Implementation Plan/Aviation Annex (AIP/Annex) to the TSSP Base Plan. Representatives from TSA and FAA co-chair the JAPWG, and an opportunity to "tri-chair" this working group will be available to the ASCC as its members become more integrated in the CIPAC process. The working group is comprised of AGCC/ASCC charter member representatives from TSA, FAA, DHS, DOT, TSA-Transportation Sector Network Management planners (Airports, Airlines, General Aviation, Cargo, and International), and subject matter experts from Cyber/Chief Information Officer and Metrics offices, among others. The JAPWG meets weekly or periodically, as required, to continue reviewing and or drafting the Aviation Implementation Plan/Annex, as required.

After the Aviation Implementation Plan/Annex was initially drafted, it was staffed out to the AGCC/ASCC, among other organizations, for review and comment. The JAPWG received comments by a certain date and the JAPWG leadership reviewed and adjudicated comments. The JAPWG leadership team will make recommendations to the AGCC/ASCC chairs if a comment is accepted, noted, or rejected, with rationale provided for any recommendation, as required. Once the TSSP and its associated Annexes (to include the Aviation Annex) are completed, it will be forwarded for TSA/DHS and FAA/DOT review and eventual submission for presidential-level approval/signature.

The Aviation Implementation Plan/Annex will follow the same formal periodic review process as the TSSP Base Plan, but will be reviewed at least annually within the AGCC/ASCC framework. The AGCC and ASCC will play essential roles in monitoring the success of each program to assess and justify continued maintenance of programs over their life cycle. The Councils will work with the appropriate security partners to ensure that this plan is reviewed and updated as necessary to ensure an effective national aviation security planning effort.

Appendix 1. Matrix of Aviation Programs

Program	Responsible Agency	Goal(s) 1,2,3
Cross Modal Programs		
Transportation Security Lessons Learned Information Sharing (LLIS)	DHS/TSA	1, 3
Homeland Security Advisory System (HSAS)	DHS	1
Continuity of Operations Program (COOP)	DHS/ALL	1, 2
Visible Intermodal Protection and Response (VIPR)	TSA	1, 2
Customs-Trade Partnership Against Terrorism (C-TPAT)	CBP/TSA	1, 3
NEDCTP Rapid Deployment Canine Team Force (NRDCTF)	TSA	1
National Capitol Region Coordination Center	TSA	1,2
National Infrastructure Coordination Center	TSA	1,2,3
Transportation Security Operations Center (TSOC)	TSA	1,2
Transportation Worker Identification Credential (TWIC)	TSA	1
NAS Infrastructure – Fixed Assets		
FAA Information Security Systems (ISS)	FAA	1, 2, 3
Facility Security Management Program	FAA	1
Visitor Vetting and Control	FAA	1
Mail and Delivery Screening	FAA	1
NAS Infrastructure – Human Capital		
HSPD-12 Joint Program Office Initiatives	FAA	1, 3
Personnel Security	FAA	1
Air Carrier/In-Flight Security Programs		
Air Traffic Security Coordinator (ATSC) / Air Defense Liaisons (ADL)	FAA/TSA	1
Aviation Worker Background Check Program (AWBCP)	TSA	1
Domestic Events Network (DEN)	FAA/TSA	1, 2
Federal Air Marshal Service (FAMS) Mission Deployments	TSA	1, 3
FAMS Force Multiplier (FAMSFM) Program		
Federal Flight Deck Officer (FFDO) Program	TSA	1
National Capital Region Coordination Center (NCRCC)	TSA	1, 2
Crew Vetting Program (CVP)	TSA	1,2
Registered Traveler	TSA	1
Secure Flight Program	TSA	1
Temporary Flight Restrictions	FAA, TSA	1, 2
Tactical Information Sharing System	TSA	1
Aircraft Operator Standard Security Program	TSA	1
Airport Security Programs		
Aircraft Operator or Foreign Air Carrier Exclusive Area Agreements	TSA	1
Airport Liaison Agent (ALA) Program	DOJ/FBI	1,2
Airport Security Area Screening (Aviation and Transportation Security Act [ATSA] 106)	TSA	1
Airport Security Consortia (Local Advisory Committee)	TSA	1
Airport Security Officer (ASO) Program	TSA	1
Airport Tenant Security Program (ATSP)	TSA	1
Homeland Security Advisory Threat Condition Enhancements (Aviation Security [AVSEC] Levels)	TSA	1
Improved Airport Perimeter Access Security (Aviation and Transportation Security Act [ATSA] section-106)	TSA	1
Investigative and Enforcement Procedures	TSA	1
U.S. Airport Emergency Plan (AEP)	TSA	1, 2
U.S. Airport Inspection Program (Annual Work Plan)	TSA	1

Program	Responsible Agency	Goal(s) 1,2,3
U.S. Airport Security Program (ASP)	TSA	1
U.S. Airports Voluntary Security Construction Guidelines	TSA	1, 3
Vendor Security Program	TSA	1
Airport Checkpoint Operations		
Backscatter	TSA	1
Document Scanners	TSA	1
Explosives Trace Detection (ETD) (Checkpoint Operations)	TSA	1
Handheld Metal Detectors (HHMD)	TSA	1
Screening of Passengers by Observation Techniques (SPOT) Program	TSA	1
Secondary Screening (Checkpoint Operations)	TSA	1
Threat Image Projection (TIP) Ready X-Ray (TRX)	TSA	1
Trace Portal	TSA	1
Walk Through Metal Detectors (WTMD)	TSA	1
Airport Checked Baggage Operations		
Approved Alternative Screening Procedures (Checked Baggage Operations)	TSA	1
Explosives Detection Systems (EDS) (Checked Baggage Operations)	TSA	1
Explosives Trace Detection Equipment (Checked Baggage Operations)	TSA	1
Secondary Screening (Checked Baggage Operations)	TSA	1
Air Cargo Inspections		
Air Cargo Freight Assessment System	TSA	1
Air Cargo Surveillance Program	TSA	1
Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)	TSA	1
Indirect Air Carrier (IAC) Revalidation Project	TSA	1
TSA Known Shipper Database Project	TSA	1, 3
General Aviation		
Airport Watch & GA Secure Hotline	TSA	1, 2
Alien Flight Student Program	TSA	1
General Aviation at Ronald Reagan Washington National Airport (GA@DCA)	TSA	1
Information Publication "Security Guidelines for GA Airports"	TSA	1
Maryland Three (MD3) Airport Inspection Program	TSA	1
Restoration of General Aviation Access to Ronald Reagan Washington National Airport (GA@DCA)	TSA	1
Private Charter Standard Security Program	TSA	1
Transportation Security Administration Access Certificate - TSAAC Protocol	TSA	1
Twelve Five Standard Security Program	TSA	1
International Programs		
Aircraft Repair Station Program	FAA/TSA	1
Foreign Air Carrier Model Security Program	TSA	1
Foreign Airport Assessment and Air Carrier Inspection Program and Automated Foreign Airport Assessment Program	FAA/TSA	1
Overseas Air Carrier Station Inspection Program	TSA	1
Counter Improvised Explosive Devices (IEDs)		
Bomb Appraisal Officer (BAO)	TSA	1
Threat Containment Unit (TCU)	TSA	1
Counter Man Portable Air Defense Systems		
Counter Man Portable Air Defense Systems (MANPADS) Vulnerability Assessment Program	FAA/TSA/FBI	1, 2