Aviation Transportation System Security Plan

Supporting Plan to the
National Strategy for Aviation Security

March 26, 2007

Aviation Transportation System Security Plan

Foreword

By issuing National Security Presidential Directive-47/Homeland Security Presidential Directive-16 (NSPD-47/HSPD-16) of June 20, 2006 ("Aviation Security Policy"), President George W. Bush established U.S. policy, guidelines, and implementation actions to continue the enhancement of U.S. homeland security and national security by protecting the United States and U.S. interests from threats in the Air Domain[1]. NSPD-47/HSPD-16 directed the development of the National Strategy for Aviation Security (National Strategy), which established the overarching framework for a comprehensive and integrated national approach to security the Aviation Transportation System, building on current successful initiatives and directing additional security enhancements where necessary, and the following seven supporting plans:

- **The Aviation Transportation System Security Plan** directs a risk-based approach to developing and implementing measures to reduce vulnerabilities within the Aviation Transportation System.
- **The Aviation Operational Threat Response Plan** prescribes comprehensive and coordinated protocols to assure an effective and efficient United States Government response to air threats against the Nation and its interests.
- **The Aviation Transportation System Recovery Plan** defines a suite of strategies to mitigate the operational and economic effects of an attack in the Air Domain, as well as measures that will enable the Aviation Transportation System and other affected critical government and private sector aviation-related elements to recover from such an attack as rapidly as possible.
- **The Air Domain Surveillance and Intelligence Integration Plan** coordinates requirements, priorities, and implementation of national air surveillance resources and the means to share this information with appropriate stakeholders.
- **The International Aviation Threat Reduction Plan** details U.S. international activities to counter illicit acquisition and use by terrorists, other criminals, and other hostile individuals or groups of stand-off weapons systems that pose the most significant threats to lawful civilian and military use of the Air Domain.
- **The Domestic Outreach Plan** ensures stakeholder participation in the implementation of the supporting plans and related aviation security policies and provides guidelines for outreach in the event of a threat to, or an attack on, the United States or another disruptive incident to the Aviation Transportation System.
- **The International Outreach Plan** provides a comprehensive framework to solicit international support for an improved global aviation security network.

While these plans address different aspects of aviation security, they are mutually dependent and complement each other. When combined with critical performance measures, collectively they create the integrated foundation essential for an effective strategy and should be regularly assessed to ensure progress in the Nation's aviation

[1] "Air Domain" is defined as the global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating, and people and cargo present in that airspace, and all aviation-related infrastructure.

security program. These plans do not alter existing constitutional and statutory authorities or responsibilities of the department and agency heads to carry out operational activities and to provide or receive information. Together, the National Strategy and its supporting plans enhance the security of the United States and its interests, including all lawful and legitimate public and private activities in the Air Domain.

Table of Contents

Executive Summary

The United States Government responded to the attacks of September 11, 2001, with an unambiguous, comprehensive increase in measures to enhance aviation security. Significant improvements were made to existing security methodologies, operations, and technologies through the creation of systems of security in each area of the Aviation Transportation System. The United States 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 United States and effectively reduced vulnerabilities within the Aviation Transportation System. Greater scrutiny has been paid to individuals in the aviation system from pilots and crew to passengers and workers on the airside. 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 our security efforts, as evidenced by the recent threats to U.S. bound flights identified by the UK.

The Aviation Transportation System Security Plan (Plan) continues, expands, and enhances efforts to further reduce vulnerabilities in all critical system areas. This Plan directs aggressive efforts to: (1) ensure that anyone entering or using the Aviation Transportation System has been identified and vetted or screened; (2) ensure the United States Government is taking all reasonable measures to detect and prevent the use of weapons against elements of the Air Domain, or to use the Aviation Transportation System to transport, become a weapon, or serve as a means of dispersal of weapons including Chemical, Biological, Radiological, Nuclear, or High-Yield Explosives (CBRNE)[2], as well as liquid explosives; and (3) harden the critical elements of the Aviation Transportation System infrastructure against other forms of attack, such as Man-Portable Air Defense Systems (MANPADS) and stand-off weapons or cyber attack.

This Plan, along with the Aviation Operational Threat Response (AOTR) and Aviation Transportation System Recovery (ATSR) plans, addresses enhancements to the national-level Air Domain prevention-response-recovery capabilities of the United States Government. As such, these three plans are aligned in function. An examination of threats, vulnerabilities, and consequences has driven the generation of this Plan's components, with designation of lead agencies to address each major element. Although the ATSS, AOTR, and ATSR are separate and distinct plans, there is an anticipation of overlap in their execution. The ATSS, focusing on measures to prevent a terrorist attack, is expected to continue in effect even if an attack occurs. The ATSS baseline measures will be in place and enhanced as appropriate to support threat response actions when and where an attack occurs, and to bolster baseline security across the entire system. Similarly, the execution of the ATSS will be in place for continuity of established security measures as recovery efforts outlined in the ATSR plan are pursued. There is also anticipated overlap between the AOTR and ATSR execution, without an expected,

[2] Chemical (C), biological (B), radiological (R), nuclear (N), and explosives (E) can be identified collectively by the acronym CBRNE, or as any sub-set thereof. For example, CB refers to chemical, biological.

definitive point where full response is completed before recovery starts. Recovery plan components will be started as soon as possible with a focus on a return to functioning, even as some response elements are continuing. If an attack should occur, coordination between plan components, and appropriateness of timing, will be key to not only to the effective execution of all three plans, but to a positive impact on the Aviation Transportation System.

Purpose

The security and economic prosperity of the Nation depends greatly upon the security of the Aviation Transportation System. The United States must prevent terrorist attacks and other criminal or hostile acts, while minimizing the impact on this system and continuing to facilitate the free flow and growth of trade and commerce. This Plan directs enhancement to the existing scalable, flexible aviation security system through development or refinement of individual security measures, as well as those for integrated systems as a whole, by more rigorously, thoroughly, and effectively assessing and addressing vulnerabilities within the Aviation Transportation System[3].

This plan, building on current security requirements and leveraging Federal authorities and expertise, is structured to ensure that efficient and effective aviation security is based on a system of shared responsibilities and costs, creating many interdependent, interlocking layers of security. Federal departments and agencies are responsible for: establishing and enforcing regulations, policies, and procedures; identifying potential threats and appropriate countermeasures; defining and mitigating risks and vulnerabilities on the ground and in the air; and applying security measures to passengers, their carry-on items, checked baggage, crewmembers, employees, and cargo. Airlines, airports, crews, law enforcement, passengers, and the shipping industry play key roles in the multi-layered protective posture that has taken aviation security beyond where it stood on September 11, 2001, and these entities will play an integral role in securing the system into the future.

This Plan does not alter existing authorities, roles, or responsibilities of the department and agency heads, but directs enhancements in these areas or pursuit of specific actions needed to address critical areas of vulnerability. This Plan reinforces the flexibility of the existing aviation security system to complement security requirements with changing threats or government adjustments in the National Threat Level. While the focus of this Plan is on preventing a successful attack through reducing vulnerabilities, the ability to prevent a wide range of events or attacks with a flexible set of protective measures enhances deterrence and system recovery by building resiliency into the Aviation Transportation System. This Plan directs the enhancement of security measures to prevent attacks and secure the Aviation Transportation System, and provides dynamic security measures to be quickly evaluated and executed, which reinforces public confidence during and after an event.

Scope

This Plan builds upon the existing scalable, flexible aviation security system through clear delineation of departmental roles and responsibilities and by directing specific actions using a risk-based approach to enhance security systems, helping to protect against continuing and significant threats to aviation. The ATSS always maintains a baseline level of security, yet is designed to be flexible enough to address the wide range of current and future threats, including the following threats identified in NSPD-

3 The Aviation Transportation System is composed of a broad spectrum of private and public sector elements, including aircraft operators, more than 19,000 private and public use airports, industry, and the National Airspace System (NAS), presenting thousands of points of entry for threats to people, aircraft or infrastructure elements.

47/HSPD-16: attacks using aircraft as weapons against ground-based targets, similar to the attacks of September 11, 2001, and including aircraft used to deliver or transport chemical weapons, biological agents, radiological dispersal devices, improvised nuclear devices, or explosives; attacks against aircraft using stand-off weapons, such as Man-Portable Air Defense Systems (MANPADS); attacks using weapons and on-board explosive devices; hijacking and air piracy; and physical and cyber-based attacks on Aviation Transportation System infrastructure. This Plan addresses these and other vulnerabilities in three broad areas: Passenger, Employee and Crew Security Assurance; Threat Object Detection/Interdiction; and Infrastructure Protection.

Strategic Goals and Objectives

This Plan supports five broad strategic actions from the National Strategy for Aviation Security:

- Maximize domain awareness
- Deploy layered security
- Promote a safe, efficient, and secure Aviation Transportation System
- Enhance international cooperation
- Assure continuity of the Aviation Transportation System

In executing the Aviation Transportation System Security plan, the United States Government will:

- Utilize a risk-based approach to define security measures that strengthen critical security systems and reduce vulnerabilities in the Aviation Transportation System.
- Employ a layered security system to prevent the Air Domain from being used by terrorist groups, hostile nation-states, and criminals to commit acts against the United States, its people, or its infrastructure.
- Develop enhancements to the security of the Aviation Transportation System that facilitate safe, secure, and efficient travel and commerce both nationally and internationally.

Guiding Principles

The following guiding principles of this Plan build on these goals:

- Effective aviation security includes a system of systems with multi-layered, individual security measures, each adding to the probability of successful prevention.
- Effective aviation security is maintained through the inclusion of randomness and unpredictability to prevent terrorist identification of our measures and create a disruption of terrorist plots and criminal acts.
- Effective aviation security is critical to global stability and economic growth and vital to the interests of the United States.
- The effectiveness of security measures must be continuously assessed and modified to reflect changes in the highly dynamic and adaptive terrorist threat.

Terrorists closely study and actively attempt to defeat our security systems. Security measures cannot remain static in methodology, application, or technological approach. Instead, they must continually evolve, with the goal of being proactive rather than reactive.

- Although the focus of this Plan is on preventing a successful attack through reducing vulnerabilities, all recommendations or plan components must take into account all three components of risk: threat, vulnerabilities, and consequences.
- The ability to prevent a wide range of events/attacks with a scalable, flexible set of protective measures will help build resiliency into the Aviation Transportation System.
- Recognition that as a multi-layered system of systems, any one of the current or recommended measures in our layered security system can potentially be compromised, but together provide greatly enhanced security. The United States Government will address, enhance, and further strengthen all major layers and systems critical to risk reduction in aviation security.
- Cooperation in the implementation of the recommended multi-layered system across all Federal departments and agencies, State, local, and tribal entities, and with our foreign partners, is essential and further enhances the strength of each measure pursued.

Roles & Responsibilities

The following are the overarching aviation security-related missions of the departments and agencies involved in the development and execution of this plan. Further details on the specific roles and responsibilities of departments and agencies are discussed within this Plan implementation section of this document.

Department of Homeland Security (DHS)

HSPD-7 assigns responsibility to DHS to coordinate protection activities for the transportation sector. DHS has assigned Sector Specific Agency responsibility to the Transportation Security Administration (TSA). Additional DHS agencies with responsibilities for components of this plan include U.S. Customs and Border Protection (CBP), Science and Technology Directorate (S&T), Federal Emergency Management Agency (FEMA), the Domestic Nuclear Detection Office (DNDO), the Office of Infrastructure Protection (OIP), and the U.S. Coast Guard (USCG).

- *TSA:* TSA has the responsibility for security in all modes of transportation, and under the guidance of relevant HSPDs/NSPDs, collaborates with DOT on transportation infrastructure protection and security issues. In addition to providing a deterrent with its National Explosives Detection Canine Team Program and a robust aviation security assessments operation, TSA provides a response capability through deployment of Federal Flight Deck Officers, Transportation Security Officers, Aviation Security Inspectors, and the TSA Explosives Operations Division. During a national emergency, TSA has the responsibility to coordinate the transportation-related responsibilities of other departments and agencies in all modes. TSA also coordinates and provides notice about threats to transportation. TSA is responsible for the vetting of passengers and aircrews flying domestically or internationally into, out of, or

within the United States, and other critical transportation populations. TSA is responsible for the vetting of all aliens, whether resident in the United States or not, applying for flight training needed to obtain, maintain, or upgrade a Federal Aviation Administration (FAA) issued airman certificate. Additionally, TSA is responsible for the vetting of other populations that may present a risk to transportation security, such as individuals with access to the secured and sterile areas of an airport and of pilots flying aircraft with a maximum take-off weight over 12,500 pounds. TSA also has responsibility for screening cargo placed aboard passenger aircraft.

- *CBP:* The primary mission of CBP is to prevent terrorists and terrorist weapons from entering the United States. CBP has the authority to stop, board, and search any conveyance crossing the U.S. border to inspect persons, cargo, mail, and documents. CBP is also responsible for detecting, identifying, and interdicting potential air threats to national security as well as conducting criminal investigations and providing case support for prosecution. CBP provides, when requested, Airspace Security enforcement to National Special Security Events and Homeland Security Events. CBP provides RADAR tracking and monitoring support to the FAA and DoD in the National Capitol Region and throughout the Continental U.S.
- *S&T:* With receipt of requirements from the responsible DHS organization, S&T conducts and enables research, development, testing, and evaluation to ensure that Federal, State, local, and private sector end users have the latest capabilities to promote homeland security.
- *FEMA:* FEMA is responsible for leading the national effort to protect public health and safety, restore essential government services, and provide emergency relief to those affected by acts of terrorism. FEMA ensures that the National Response Plan is adequate to respond to the consequences of terrorism.
- *DNDO:* DNDO, in conjunction with other agencies, is responsible for developing and implementing the domestic nuclear detection architecture to detect and report unauthorized attempts to improperly possess, store, develop, or transport nuclear or radiological materials. This includes ensuring linkages of detection capabilities across Federal, State, territorial, tribal, and local agencies.
- *OIP:* OIP will ensure a safe, secure, and resilient national infrastructure (including aviation) through public and private partnerships. OIP will lead the coordinated national effort to reduce the risk to our critical infrastructures and key resources posed by acts of terrorism, and strengthen national preparedness, timely response and rapid recovery in the event of an attack, natural disaster or other emergency. To accomplish this mission the OIP must: understand and share risk and other information about terrorist threats and other hazards to our national Critical Infrastructure and Key Resources (CI/KR); build and sustain effective CI/KR partnerships and coordination mechanisms; build and implement a sustainable, national CI/KR risk-management program; ensure efficient use of resources for CI/KR risk reduction; and, provide a foundation for continuously improving national CI/KR preparedness.
- *USCG:* Acting through the U.S. Coast Guard, conducts aviation operations in support of National Defense, law enforcement, and National Security, including National Defense in the National Capital Region.

Department of Transportation (DOT)

The Department of Transportation has broad responsibility for promoting and maintaining the safety and efficiency of the entire U.S. transportation system. The Department's Federal Aviation Administration has specific authorities over and responsibilities for the regulatory oversight and operation of the National Airspace System (NAS) as the country's civil aviation authority and air navigation services provider. DOT/FAA also has national defense and homeland security authorities and responsibilities, under which it works in partnership with DHS, DOD, and other aviation security stakeholders.

- *FAA:* The FAA regulates and operates the NAS and continues to be the sole authority for airspace management, aviation regulations, and airspace usage, although the FAA works closely with TSA and other partners on aviation security matters, as appropriate. In circumstances that potentially affect the national defense or homeland security, FAA, in consultation with DoD, DHS, and other partners, establishes needed airspace restrictions and other air traffic management measures. The FAA also has specific responsibilities and authorities relating to safety and security of critical NAS infrastructure, as well as responsibility for providing technical advice and regulatory certification for aircraft-based attack countermeasures.

Department of Justice (DOJ)

The mission of the DOJ is to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide Federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans. As the investigative arm of DOJ, the Federal Bureau of Investigation (FBI) has been designated as the lead Federal agency to investigate terrorism.

The FBI has multiple programs and initiatives related to aviation security. The FBI's Civil Aviation Security Program (CASP) supports and enhances the FBI's efforts to prevent, disrupt, and defeat terrorist operations directed toward civil aviation and provides counterterrorism preparedness leadership and assistance to Federal, State, and local agencies responsible for civil aviation security. The mission of CASP is carried out primarily through the Airport Liaison Agent (ALA) Program that includes over 500 designated ALAs who are responsible for maintaining liaison relationships at the approximately 450 TSA-regulated airports. The duties of ALAs include responding to aviation-related incidents, investigating threats, interviewing people on Terrorist Watch Lists, participating in Joint Airport and MANPADS Vulnerability Assessments (MVAs), participating in the planning and execution of training exercises, and developing liaison with aviation industry stakeholders.

Department of Defense (DoD)

DoD is responsible for deterring, defending against, and, if necessary, defeating aviation threats, including nation-state threats, to the United States and its interests globally. DoD, through NORAD and the Combatant Commands, as appropriate, conducts deterrence and prevention activities and prepares for operational response through

employment of significant numbers of fighter aircraft on ground alert, ground-based missile defense systems in the National Capital Region and other areas, as warranted, and airborne fighter patrols throughout the United States. These assets are employed at the direction of senior DoD commanders using a tiered, graduated system that accounts for threat conditions and identified vulnerabilities. DoD is responsible for protecting the civilian assets and commercial crewmembers assigned to the Civil Reserve Air Fleet. Additionally, DoD is prepared to conduct defense support of civil authorities as directed by the President or the Secretary of Defense.

Department of State (DOS)
DOS is responsible for leading international outreach and coordination with foreign governments for enhanced cooperation in the Air Domain, including data transfer, and other international advance passenger screening.

Department of Commerce (DOC)
DOC has broad responsibilities for providing aviation industry and trade policy expertise in interagency policy development efforts and international negotiations, and economic and industry analysis of the impact of domestic regulations (including security-related regulations) and international trade agreements. DOC engages in cooperative efforts on aviation trade and security issues in numerous international bodies and fora, including the International Civil Aviation Organization, the Security and Prosperity Partnership with Canada and Mexico, the World Trade Organization, and the Asia Pacific Economic Cooperation forum. DOC provides the scientific and technical expertise necessary to measure and verify that devices, equipment, and technologies meet or exceed the requirements necessary to maintain and advance the security of the Air Domain. DOC promotes the development of metrology, performance and physical standards, measurement science, and test and evaluation programs that support the development of devices, equipment and technologies. DOC provides weather forecast and analysis services integral to the operations of the Aviation Transportation System DOC also manages radio frequency spectrum allocation among federal agencies, including for emergency situations.

Office of the Director of National Intelligence (ODNI)
The Director of National Intelligence is responsible for overseeing efforts by the Intelligence Community – including through signals, imagery, and human collection – to provide all-source assessments of how terrorists and other adversaries and criminals are seeking to defeat Aviation Transportation Security measures.

Interagency Implementation Requirements

Each day, airports process millions of passengers and thousands of tons of cargo. There are an estimated 900,000 workers who perform duties in the secured areas of our airports. It is estimated that there are more than 5,600 public-use general aviation airports in the United States in addition to the more than 450 commercial airports staffed with the TSA screening workforce. The Air Domain contains thousands of critical infrastructure elements that, if disrupted, create ripple effects throughout the entire Aviation Transportation System. Terrorists are known to have considered the aviation system and its elements as targets for attack, both direct and indirect. The United States Government

must continue to address vulnerabilities to create resiliency against current and evolving threats using individuals and all forms of weapon systems or targeting any component of the infrastructure. Following are directed actions to further enhance the security of the United States and U.S. interests, as well as protection of the Aviation Transportation System through enhancements to the system itself. Any budgetary requirements resulting will be addressed within the context of agency, departmental, and government-wide budgetary decision-making processes.

Passenger, Employee, and Crew Security Assurance

Given the millions of passengers, thousands of pilots and crewmembers, and hundreds of thousands of Aviation Transportation System workforce members accessing the NAS and other areas of the Aviation Transportation System every day, it is imperative that all individuals using and working within that system are adequately and effectively identified and appropriately screened. While there are obvious challenges to ensuring confidence in the passengers boarding our aircraft, even broader challenges exist for those who access the system, such as the employees, contractors, sub-contractors, and crewmembers working in the terminal and Airport Operations Area.

Departmental Requirements

Department of Homeland Security will:

- Assume the responsibility for vetting international and domestic air passengers and crew against the No-Fly and Selectee Lists.

- Align the regulatory and information technology requirements for a DHS pre-departure, name based, passenger pre-screening system. This system will cover both domestic and international passenger and crew vetting.
    - Implement the collection of international passenger data pre-departure with a target date of early Fiscal Year 2007.
    - Implement Secure Flight by December 31, 2008.

- Coordinate consolidation of all interagency redress programs by the end of Fiscal Year 2007.

- Explore the feasibility of upgrading secured area access controls through the implementation of measures such as adding biometric identifiers to employee credentials, as well as enhancing physical security programs and measures to apply to all airport employees and vendors.

- Assume responsibility for verification of passenger identity and deploy behavior observation techniques at and beyond the checkpoint.

Department of Justice will:

- Expand the screening network to include foreign information sharing, in coordination with DOS and appropriate departments and agencies.

- Consolidate Watch List data and vetting processes to ensure consistency, integrity, and security and, in cooperation with contributing agency partners, ensure the Terrorist Screening Database is thorough, accurate, and current.

Department of State will:

- Negotiate agreements with foreign nations (or multi-national organizations) to obtain access to passenger data for persons traveling to the United States prior to aircraft takeoff, in coordination with DHS.

Recommendations for Statutory, Regulatory, Organization, or Policy Changes

DHS, in coordination with DOS and DOT, will explore the legislative and diplomatic feasibility, consistent with international obligations, of vetting manifests for aircraft overflying the territorial airspace of the United States.

DOJ, DOS, and DHS will ensure new policies and regulations provide for strict privacy controls on all personally identifiable data to protect it from misuse or unauthorized disclosure.

Threat Object Screening and Detection

The use of explosives to target major population centers, critical U.S. infrastructure, or aircraft and infrastructure within the Aviation Transportation System is a continuing threat. The knowledge and capability of hostile nations and the continuing desire of terrorist groups to develop and deploy CBRNE weapons is also of the utmost concern. The Nation must also look beyond the historical approach used by terrorists to introduce weapons into the system and cannot assume that threat objects will only be on the person or in carry-on or checked baggage. The cargo system, for example, has an extensive supply chain with multiple potential points of entry requiring a comprehensive, layered security approach.

Departmental Requirements

Department of Homeland Security will:

- Continue to develop, improve, and augment CBRNE detection screening systems at the checkpoint and for hold baggage, as well as explore new on-board aircraft detection, identification, containment, and mitigation technologies, in coordination with the research and development community, DOT, and stakeholders.

- Continue to research automated hold baggage CBRNE detection systems that accurately and efficiently detect the amount, types, and configurations of threat materials.

- Assess future checkpoints that could be system engineered as individual operating units with modularized, quickly interchangeable detection units, so as to be easily modified to accurately detect the changing range of threats while, at the same time, minimizing the checkpoint "footprint," and providing for removal and servicing of

units with minimal disruption of the screening function. Checkpoints should be qualified as integrated systems.

- Deploy in-line explosive detection systems for carry on bags at the checkpoint.

- Engage in additional research on other terrorism tactics that may be used to breach secure areas on the aircraft, including research on small explosives charges.

- Work toward enhancing and harmonizing the checked baggage screening processes on flights from Canada to the United States, potentially using a combination of additional processes or technologies to bridge U.S. and Canadian standards. These opportunities should be explored through the Security and Prosperity Partnership process, and in collaboration with DOS.

- Seek to harmonize passenger and baggage screening internationally.

- Collaborate with DOT to develop and implement a strategy to counter CBRNE attacks on Aviation Transportation System facilities, including airports and critical NAS facilities.

- Strengthen security vetting of shipper and supply chain sources and enhance physical security of cargo in transit by improving the Indirect Air Carrier Security Program and Customs-Trade Partnership Against Terrorism.

- Continue collaboration to leverage existing and developing infrastructure and technology to identify international elevated risk cargo through prescreening and to identify, develop, and deploy technology, canines, and procedures for performing 100 percent inspection of targeted cargo.

- Establish national explosive detection canine standards and expand canine coverage throughout the aviation transportation system.

- Enhance the Automated Commercial Environment by using the Advanced Trade Data Initiative to acquire additional supply chain information to identify all parties involved in international shipments, check the accuracy of reported information, and leverage technology to improve current government and industry processes to disseminate information.

- Create and maintain a validated threat and risk assessment document for the Aviation Transportation System, determine aviation sector requirements for dealing with CB threats, coordinate with other agencies dealing with the same threat, and create guidance to help aviation facilities and aircraft operators develop a threat mitigation strategy, in partnership with other Federal, State, local, tribal, and private sector stakeholders.

- Develop an evaluation system for assessing the individual and combined effectiveness of layered approaches to aviation security.

- In coordination with other appropriate agencies, lead a national effort to synchronize the development of CBRNE detection capabilities in the Air Domain.

Recommendations for Statutory, Regulatory, Organizational, or Policy Changes

The Trade Act of 2002 provides CBP with the ability to require advance electronic cargo manifest information. Currently, this is implemented by requiring the information at "wheels up" or four hours prior to arrival in the United States. CBP, in coordination with DOS and DOT, will explore changing implementation of this enhanced risk assessment system by increasing the advanced notice period.

Protection of the Aviation Transportation System Operational & Infrastructure Elements

Securing U.S. airspace and the Aviation Transportation System infrastructure against threats, violations, attacks, and other disruptions, such as cyber attack or disabling of remotely located resources, requires not only multiple layers of protection but multiple agencies working cooperatively and in a coordinated fashion. On-ground infrastructure elements of the Aviation Transportation System are critical to continued safety and security services necessary to support air operations in U.S. airspace and are dependant on solid security measures.

There is also a potential threat against U.S. assets by more remote stand-off weapon systems such as MANPADS that must be regularly reviewed and updated to address their world-wide presence and regular use. New technologies, policies and procedures must be continually pursued to address these threats.

Departmental Requirements

<u>Department of Homeland Security will:</u>

- Continue to improve coordination of crew and passenger vetting for all flights into or out of U.S. territorial airspace, including general aviation, in coordination with DOS.

- Review Notice to Airmen (NOTAMs) dealing with airspace security and explore the feasibility of the establishment of security programs for all U.S. registered general aviation aircraft, in coordination with DOT.

- Counter the domestic smuggling of, and illicit access to, MANPADS and other stand-off weapons that pose significant risks to domestic aviation, as well as opportunities for use of those weapons against aircraft.

- Continue the program of assessments of domestic airport's vulnerabilities to MANPADS and expand the program assessing the vulnerability of foreign airports to attacks from MANPADS.

- Continue to explore the development of cost-effective systems for commercial aircraft, including examination of existing military technologies and continued technology assessment, demonstration, and validation programs for countermeasures commensurate with the threat and evolving technologies of MANPADS.

- Develop security criteria thresholds for designation of flights of interest.

- Increase the ability to detect and monitor all aircraft entering U.S. territorial airspace, including general aviation.

Department of Transportation will:

- Enhance security measures to protect critical NAS infrastructure such air traffic control facilities and systems from both physical and cyber attacks.

- Explore with DHS/TSA and other key partners strategies to strengthen procedures to authorize only those international flights, including general aviation, into U.S. airspace that have been vetted and pre-approved according to pertinent security regulations. DOT will lead this effort with regard to air navigation services considerations for such assess, including system safety and efficiency, in cooperation with the Department of Homeland Security, which will lead the effort for matters relating to security.

- Continue to enhance the capability to dynamically reconfigure airspace in response to short-notice security requirements.

- Continue to enhance the capability to develop, implement, and manage airspace and air traffic management related security measures that are scalable and flexible to support steady-state security requirements, as well as operational threat response and recovery efforts, in coordination with DHS, DoD, and other aviation security partners.

- Continue to explore the development of improvements to the current NOTAM system, which will enhance the system's ability to support specific needs of security NOTAMs, including accelerated release.

- In coordination with DHS/TSA and other partners, DOT/FAA will continue to explore the development of an enhanced tracking system that monitors enforcement actions and sanctions for security related airspace violators across the United States in order to ensure consistency of sanctions taken against pilots, monitor trends, and if possible predict future violations and to ensure prompt imposition of appropriate sanctions on airspace violators to serve as a deterrent to others.

- Support DHS and DoD aviation security and defense activities, as a full aviation security partner, through airspace restructuring, aircraft diverts, ground delays and stops, or other air traffic management and security strategies.

- Continue to explore, in cooperation with DHS/TSA and other key partners, strategies to improve capabilities that better enable flexible access to select restricted airspace by vetted aircraft and crew.

- Continue to explore, in coordination with DHS/TSA and other key partners, strategies to further improve the ability to use and integrate flight data and other information regarding aircraft and air operators for situational awareness and real time security operations.

- Continue to explore, in coordination with DHS/TSA, the Joint Program Development Office (JPDO), and other key partners, strategies to identify and leverage communications, navigational aids, and surveillance systems used within the NAS to further strengthen aviation security capabilities.

Department of Defense will maintain a state of readiness and protective posture to ensure the security of DoD infrastructure and information related to the Aviation Transportation System and DoD air defense assets, in addition to those responsibilities noted earlier.

Department of Justice will maintain a community cooperation program and the sharing of threat information enabling an effective response effort.

Department of State will assist foreign governments in their efforts to strengthen controls over MANPADS stock and to prevent the illicit trade and trafficking of MANPADS. DOS will continue to pursue efforts toward nonproliferation of MANPADS and other stand-off weapons.[4]

Office of the Director of National Intelligence will, in coordination with DHS, DOJ, and DOT, establish intelligence indicators and warning criteria for MANPADS and other stand-off weapons attacks.

Interagency

Each of the following interagency activities will align with the JPDO Next Generation Air Transportation System enterprise architecture and concept of operations. By maintaining this alignment, DOT, DHS, and DoD will jointly ensure a cost effective and consistent evolution and implementation path of these aviation security programs.

- DHS, DoD, and DOT will continue the development of technological and procedural measures to detect, prevent, respond to, and recover from physical and cyber-based attacks against Aviation Transportation System critical infrastructure, and will increase coordination between the government and the private sector to achieve an integrated protective system for all critical infrastructure elements of the Aviation Transportation System.

[4] These and other international activities to prevent the illicit acquisition and use of MANPADS and other stand-off weapons systems are addressed in the International Aviation Threat Reduction Plan.

- DHS, DoD, and DOT will conduct a comprehensive risk assessment and develop a research, development, testing, and evaluation program to address cyber, radio frequency, and electromagnetic pulse attacks.

- DHS, DOJ, DOT, and other stakeholders will develop protocols and plans for coordinating interagency efforts to develop, establish, maintain, and validate steady-state security measures to guard against MANPADS and other stand-off weapons. These protocols and plans should leverage ongoing MVAs and MANPADS Mitigation Plan efforts by DHS, and should be harmonized with operational response plans developed under the AOTR plan.

Recommendations for Statutory, Regulatory, Organization, or Policy Changes

DOT/FAA will explore the feasibility of establishing new rulemaking and related regulatory tools that would reinforce the current requirements for pilots to use their aircraft's legal registration number or call sign, and allow for enforcement action if they do not comply. DOT/FAA will pursue a similar investigation with regard to establishment of security airspace measures.

Conclusion

The effective implementation of the security measures in the Aviation Transportation System Security plan requires cooperation and information-sharing among Federal, State, local, and tribal agencies, as well as industry and foreign partners. In addition, funding and resources must be allocated to maintain and enhance current security measures, and resources must be available to research and employ new measures as appropriate.

While this plan was developed in coordination with the Aviation Operational Threat Response and Aviation Transportation System Recovery plans, it is only through the synchronized implementation of these three foundational plans that the United States Government will be able to effect the active, layered security and defense in depth that is necessary to protect the United States and its interests from terrorist and criminal acts and other hostile attacks.