Order Code RL34302

CRS Report for Congress

National Aviation Security Policy, Strategy, and Mode-Specific Plans: Background and Considerations for Congress

January 2, 2008

Bart Elias
Specialist in Aviation Policy
Resources, Science, and Industry Division

Congressional Research Service

Prepared for Members and Committees of Congress

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
02 JAN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
National Aviation Security Policy, Strategy, and Mode-Specific Plans: Background and Considerations for Congress	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,The Library of Congress,101 Independence Avenue, SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

National Aviation Security Policy, Strategy, and Mode-Specific Plans: Background and Considerations for Congress

Summary

In the years leading up to the terrorist attacks of September 11, 2001, the United States lacked a comprehensive national policy and strategy for aviation security. The approach to aviation security was largely shaped by past events, such as the bombing of Pan Am flight 103 in December 1988, rather than a comprehensive evaluation of the full range of security risks. The 9/11 Commission concluded that the terrorist attacks of September 11, 2001 revealed failures of imagination, policy, capabilities, and management by both the FAA and the U.S. intelligence community.

Following the September 11, 2001 attacks, U.S. aviation security policy and strategy was closely linked to the changes called for in the Aviation and Transportation Security Act (ATSA, P.L. 107-71), which emphasized sweeping changes to the security of passenger airline operations. While the importance of strategic planning was recognized, it was not a priority. The 9/11 Commission Report concluded that the TSA had failed to develop an integrated strategy for the transportation sector and mode specific plans, prompting Congress to mandate the development of these strategies and plans in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). While the TSA has developed these strategies and plans, the documents have been considered security sensitive thus limiting public discourse on the DHS strategy for aviation security. However, in June 2006 President Bush directed the DHS to establish and implement a national strategy for aviation security and an accompanying set of supporting plans.

Under the framework for national aviation security policy established by the President, the DHS has developed a publicly-available national strategy for aviation security that addresses threats to aviation using a risk-based methodology to complement the overarching National Infrastructure Protection Plan (NIPP) and seeks to deter and prevent terrorist attacks against aviation, mitigate damage and expedite recovery and minimize the impact of an attack to the aviation system. The strategy seeks to achieve these objectives by engaging domestic and international partners and carrying out specific actions set forth in a series of supporting plans for operational security, surveillance and intelligence, threat response, system recovery, and coordination.

Congress may have a specific interest in assessing whether these plans are comprehensive, adaptable, sustainable, and adequately coordinated with budgetary decisions and resource allocation. Specific issues for Congress may include the validity of the strategy's underlying risk assumptions; the extent to which 9/11 Commission recommendations and statutory requirements are reflected in the strategy; consideration of sustainability of and advancement of security technologies to meet future needs and system demands; whether the strategy is sufficiently forward-looking and not reactive in its approach; the extent to which the strategy provides a comprehensive framework for a robust aviation security system; and the degree to which strategic objectives and approaches align with budget priorities and resource availability. This report will not be updated.

Contents

List of Figures

National Aviation Security Policy, Strategy, and Mode-Specific Plans: Background and Considerations for Congress

Background

In the years preceding the terrorist attacks of September 11, 2001, the United States lacked a comprehensive national policy and strategy for aviation security. The United States approach to aviation security had largely been shaped by past events such as the bombing of Pan Am flight 103 in December, 1988 and, at that time, was undergoing a reactive shift in strategy, placing emphasis on addressing the threat of aircraft bombings aboard commercial airliners, albeit with limited resources and a much slower time frame compared to actions taken following the terrorist attacks of September 11, 2001.

In April 2001, the Federal Aviation Administration issued a strategic plan for civil aviation security titled "A Commitment to Security." The vision was for the FAA and the U.S. aviation security system to be "[r]ecognized as the world leader in civil aviation security — identifying and countering aviation-related threats to U.S. citizens worldwide."[1] The strategic goal stated in the plan was to let "[n]o successful attacks against U.S. civil aviation" occur.[2] In comparison to the breadth and depth of the post-9/11 focus on aviation security, the desired key results stated in this document in retrospect seem quite modest and the goal tragically unattained. The pre-9/11 strategic plan sought to improve on checked baggage and checkpoint screening performance and utilize a combination of explosives detection system (EDS) screening and positive passenger baggage match (PPBM) techniques to vet 100% of checked baggage. In addition to improving technical capabilities to detect explosives in checked baggage, strategies identified by the FAA included

- establishing security screening operations and training standards which, at that time, did not exist;
- ensuring Federal Air Marshals were available to protect selected high-risk flight, although their numbers had dwindled to 33 at the time of the 9/11 hijackings;[3]

---

[1] Federal Aviation Administration, *A Commitment to Security, Civil Aviation Strategic Plan 2001-2004*, April 2001, p. 3.

[2] Ibid., p. 11.

[3] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Authorized Edition), New York, NY: W.W. Norton & Company , p. 85.

- ensuring that certified explosives canine teams were available at major U.S. airports; and
- ensuring preparedness and crisis management to respond to incidents that may occur.

The FAA Civil Aviation Security Strategic Plan also sought to improve air cargo security, primarily to reduce transport of dangerous goods, a likely response to the concerns over the transport of dangerous goods highlighted by the May 11, 1996 crash of Valujet flight 592 in the Florida Everglades. The strategic plan sought to achieve this objective largely through industry training and education and targeted inspections of dangerous goods transportation areas. Despite the emphasis on preventing aircraft bombs carried in passenger luggage, the potential threat of a bomb placed in air cargo was not mentioned in the strategic plan. Also, while the strategic plan addressed internal FAA security, the emphasis of this strategic element was on handling and protection of sensitive information and maintaining up-to-date background checks and clearances for employees in security-sensitive positions. While the strategic plan did identify the completion of facility security assessments and the protection of information systems among key results sought, it did not convey any insight regarding the potential threats and vulnerabilities of air traffic facilities to physical attack or FAA information systems to physical or cyber-attack.

The FAA's pre-9/11 strategic plan also identified several key results regarding external relationships including improved communications with Congress, the aviation industry, foreign governments, the Office of Management and Budget (OMB), and the Department of Transportation, Office of Inspector General (DOT OIG). The strategic plan, however did not specifically address relationships with federal law enforcement agencies and the intelligence community, factors that became a central focus of post-9/11 homeland security policy debate. The strategic plan also did not address relationships and coordination with the military for incident response, a major deficiency in the FAA's response to the hijackings on September 11, 2001, and an area of considerable focus during post-9/11 strategic planning.

While the FAA strategic plan for aviation security failed to adequately consider all security risks, the 9/11 Commission concluded that the terrorist attacks of September 11, 2001, revealed failures in imagination, policy, capabilities, and management both on the part of the FAA and the U.S. intelligence community. Although the brunt of the criticism levied by the 9/11 Commission was directed at the U.S. intelligence community, it faulted the FAA for focusing too heavily on the threat of bombings and for not involving the FAA's civil aviation security intelligence functions in the FAA's policymaking process. The 9/11 Commission pointed out that the suicide hijacking threat was imaginable, and was, in fact, imagined by FAA Civil Aviation Security intelligence analysts in 1999, but largely dismissed as being unlikely.[4] The 9/11 Commission faulted Congress as well for becoming entrenched in debate over airline passenger service issues while failing to focus attention and resources on the terrorist threat to the aviation system. The FAA Civil Aviation Security Strategic Plan released in April 2001serves as evidence that the FAA did not create a comprehensive strategy for protecting the aviation domain

[4] Ibid., p. 345.

from the full spectrum of terrorist threats, and did not effectively prioritize and allocate resources for reducing the vulnerability of the aviation system to possible terrorist attacks.

Immediately following the terrorist attacks of September 11, 2001, aviation security policy and strategy debate were closely linked to the legislative process leading to the swift passage of the Aviation and Transportation Security Act (ATSA, P.L. 107-71). With regard to strategy and policy, ATSA gave the newly created position of Undersecretary of Transportation for Security (now known as the TSA Administrator) specific authority and responsibility for assessing threats to transportation and developing policies, strategies, and plans for dealing with these threats to transportation security.[5] However, the primary emphasis of ATSA was on the security of passenger airline operations, and the immediate focus of the TSA was to meet congressionally established requirements and deadlines for the deployment of air marshals, the federalization of airport security screeners, and 100% explosives detection system (EDS) screening of checked baggage. While the importance of establishing comprehensive policy and strategy for aviation security was recognized by many policymakers, a strategic plan for protecting the aviation domain was slow to take shape.

In 2002, as these mandates for enhancing passenger airline security set forth in ATSA were being carried out, and while Congress debated legislation to establish the Department of Homeland Security (DHS), the Bush Administration began examining U.S. policies for protecting the homeland against future terrorist attacks in a broader context, considering other infrastructure and assets beyond the aviation domain that may be at risk. In July 2002, the President issued the National Strategy for Homeland Security and in February 2003, the President issued the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. However, neither of these strategies offered specific details on aviation security strategy, nor did they specify how aviation security plans and programs fit into these broader strategies for protecting the homeland and its critical infrastructure and key resources (CI/KR) from terrorist attacks.

On July 22, 2004, the 9/11Commission released its final report, concluding that the TSA had failed to develop an integrated strategic plan for the overall transportation sector and specific plans for each of the transportation modes. The 9/11 Commission recommended that the U.S. strategy for transportation security should be predicated on a risk-based prioritization for allocating limited resources to protect transportation infrastructure in a cost-effective manner, assigning roles and responsibilities for federal, state, regional and local authorities as well as private stakeholders.[6] Following the release of the 9/11 Commission's final report, Congress made addressing the recommendations of the report a key legislative priority, reflecting many of the commission's recommendations in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) which was enacted on December 17, 2004. The act specifically required the DHS to develop, prepare,

---

[5] See Title 49 U.S.C. § 114.

[6] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, p. 391.

implement, and keep up-to-date a comprehensive national strategy for transportation security and mode-specific security plans. Reflecting 9/11 Commission recommendation language, the act required the strategy to assign risk-based priorities and realistic deadlines for implementing practical and cost-effective defenses against security threats, setting forth agreed upon roles and missions for federal, state, regional, and local authorities and mechanisms for private sector cooperation and participation.

Under the requirements established in the act, the National Strategy for Transportation Security was to be accompanied by mode-specific security plans, including an aviation mode-specific plan. The modal security plan for aviation was required to include a threat matrix outlining each threat to the United States civil aviation system and the corresponding layers of security in place to address these threats and a plan for mitigation and reconstitution of the aviation system in the event of a terrorist attack. While the act required that the first iteration of the strategy be transmitted to the congressional homeland security authorizing committees[7] by April 2005, the strategy document was delivered in September 2005. As required by law, updates to the strategy and the mode-specific plans must be transmitted to Congress every two years. These strategy documents have been designated as security sensitive information as provided for in the act. Consequently, they have had limited distribution beyond the DHS and the homeland security authorizing committees in Congress. Therefore, there has not been extensive public discourse on the DHS approach to developing a national strategy for transportation security and strategies and plans specific to protecting the aviation mode from future terrorist attacks.

However, in June 2006, President Bush issued policy guidance directing the DHS to establish and implement a national strategy for aviation security and a series of supporting plans for implementing this strategy.[8] Unlike prior strategies and plans that had either been too broad in scope to provide detailed information regarding aviation-specific security strategies or were limited in distribution, the policy, strategy, and supporting plans developed under this Presidential directive have been made available to the public, thus offering insight into the strategic direction and approach to aviation security being pursued by the DHS in coordination with other federal agencies. These documents are also much more comprehensive in their consideration of security in the aviation domain compared to prior strategy documents and therefore provide a more thorough picture of U.S. policy and strategy for mitigating threats involving aviation. This report examines the current National Aviation Security Policy, the National Strategy for Aviation Security, and formal mode-specific plans developed for implementing this strategic approach. This report also identifies and discusses some overarching considerations for congressional oversight and possible legislative action regarding the U.S. policy and strategy for securing the aviation domain.

---

[7] At present, the congressional committees having primary jurisdiction over the Department of Homeland Security are the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs.

[8] President George W. Bush, *National Security Presidential Directive/NSPD-47, Homeland Security Presidential Directive/HSPD-16, Subject: Aviation Security Policy*, Washington, DC: The White House, June 20, 2006.

National Aviation Security Policy

The National Aviation Security Policy represents the overarching aviation-specific components of The National Strategy for Homeland Security. That strategy specifies that the Department of Homeland Security (DHS) will serve as the focal entity for managing and coordinating border and transportation security initiatives "... to prevent the entry of terrorists and the instruments of terror, while facilitating the legal flow of people, goods, and services on which our economy depends."[9] The policy, however, addresses a broader spectrum of threats to the air domain that include not only specific threats to the homeland, but also threats to national security interests both within the United States and abroad. Therefore, in addition to the overall responsibility for homeland security and aviation security for which the DHS and the TSA are directly responsible, the National Aviation Security Policy also involves matters concerning the Department of Defense, the Department of State, the Department of Justice, and a variety of other federal, state, and local agencies and private entities, and relies on close coordination with and continued cooperation from other nations.

On June 20, 2006, President Bush issued Homeland Security Presidential Directive 16 (HSPD-16/ National Security Presidential Directive 47 (NSPD-47)) establishing new U.S. policy, guidelines, and implementation of actions to address threats to the air domain. The document broadly defines the air domain as the global airspace and all aircraft operating within that airspace including both manned and unmanned vehicles, as well as all people and goods being transported by such aircraft, and all supporting aviation infrastructure.

The policy objectives set forth in HSPD-16 endeavor to prevent terrorist acts and other hostile actions either directed at or exploiting elements of the aviation domain while also minimizing the impact on air commerce and fostering the economic growth and stability of the aviation industry. The statement of policy notes that:

> [t]he United States must continue to use the full range of its assets and capabilities to prevent the Air Domain from being used by terrorists, criminals, and other hostile states to commit acts of terrorism and other unlawful or hostile acts against the United States, its people, property, territory, and allies and friends, all while minimizing the impact on the Aviation Transportation System and continuing to facilitate the free flow and growth of trade and commerce in the Air Domain. These efforts are critical to the global stability and economic growth and are vital to the interests of the United States.[10]

---

[9] White House Office of Homeland Security, *National Strategy for Aviation Security*, July 2002, p. 22.

[10] President George W. Bush, *National Security Presidential Directive/NSPD-47, Homeland Security Presidential Directive/HSPD-16, Subject: Aviation Security Policy*, Washington, DC: The White House, June 20, 2006, p. 3.

The stated policy specifies that the United States, in cooperation with international partners, will take all necessary and appropriate actions, consistent with applicable laws, statutes, and international agreements, to enhance the security and protect the United States and U.S. interests in the air domain. The implementation of this policy is to be consistent with a risk-based prioritization of aviation security strategies and tactics. Activities to support this policy objective specifically cited in this directive include

- protecting critical transportation networks and infrastructure from terrorist attacks and other hostile, criminal, and unlawful acts and reducing the vulnerability of the air domain to these types of possible attacks or exploitation;
- improving situational awareness of security issues affecting the air domain and facilitating and enhancing information sharing to improve detection of threats and appropriate responsive actions;
- ensuring seamless, coordinated efforts relating to aviation security among federal, state, tribal, and local agencies and authorities;
- enhancing the resilience of the air transportation system to a terrorist attack, including the capability to rapidly recover from such an attack and minimize impacts on economic, transportation, social, and governmental systems;
- countering the proliferation of standoff weapons, such as shoulder-fired missiles, that pose significant risks to both civilian and military users of the air domain by terrorists, criminals, and other hostile groups and individuals; and
- enhancing international relationships and promoting the integration of other nations and private sector partners in an improved global aviation security framework.

Implementation of this policy is to be coordinated through the President's Homeland Security Council (HSC) Border and Transportation Security Policy Coordination Committee (BTS PCC). The policy established a requirement for the Secretary of Homeland Security to develop an overarching national strategy for aviation security and supporting plans to carry out this strategy.

The National Strategy for Aviation Security

HSPD-16 directed the Department of Homeland Security to implement this policy through the creation of an overarching national strategy for aviation security. The directive explicitly called for the development of a national strategy for aviation security that is adaptive to changing threat levels and types of threats, and it is rooted in a risk-based, multi-disciplinary, and global approach to aviation security. The directive required that the national strategy, along with its supporting plans, include, at a minimum, risk-based approaches to address the following threats:

- attacks using aircraft against ground-based targets, including possible attacks using aircraft to deliver or transport chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons;

- attacks using stand-off weapons, such as shoulder-fired missiles or other man-portable air defense systems (MANPADS);
- attacks using on-board explosive devices and other conventional and non-conventional weapons to directly target aircraft;
- hijackings and air piracy; and
- physical attacks or cyber-attacks on aviation critical infrastructure and facilities, such as air traffic control facilities and networks and navigation systems.

The directive also identifies several specific action items to be addressed in supporting mode-specific plans to implement the national strategy for aviation security. The required plans include

- the Aviation Transportation System Security Plan;
- the Aviation Operational Threat Response Plan;
- the Aviation Transportation System Recovery Plan;
- the Air Domain Surveillance and Intelligence Integration Plan;
- the International Aviation Threat Reduction Plan;
- the Domestic Outreach Plan; and
- the International Outreach Plan.

The National Strategy for Aviation Security, along with several of these supporting plans (except for the Aviation Transportation System Recovery Plan which is still undergoing internal review within DHS and the International Aviation Threat Reduction Plan), was publically released on March 26, 2007.

Threats to Aviation

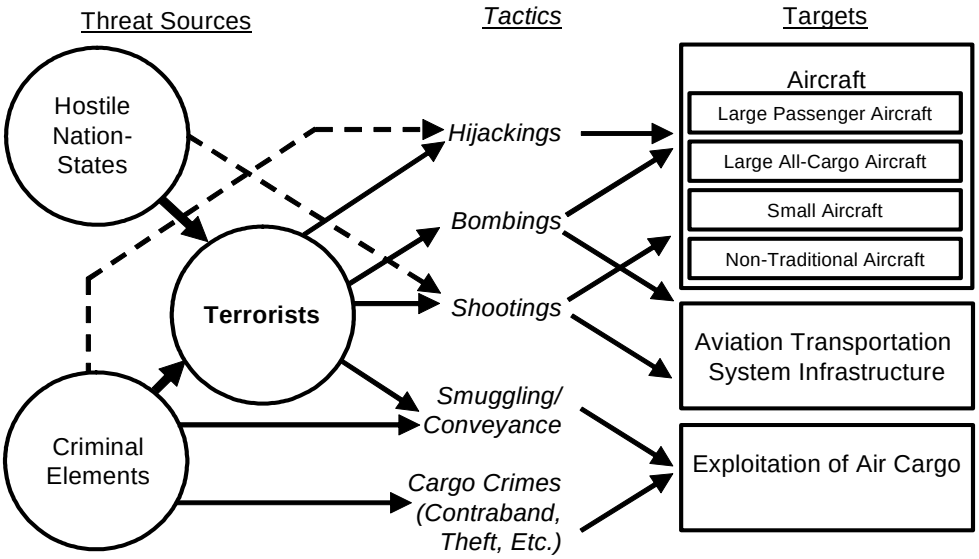
The National Strategy for Aviation Security identifies three origins or sources of threats to the air domain: terrorist groups, hostile nation-states, and criminals. The strategy document points out that while physical attacks from terrorist groups pose the most prominent threat, terrorists may also use criminal tactics to move operatives, weapons, explosives or possibly weapons of mass destruction (WMDs) through the aviation system. The strategy notes that "[s]uch threats are particularly worrisome in areas of the world where governments are weak or provide safe haven to terrorists."[11] Further, hostile-nation states may directly sponsor international terrorism directed against aviation by providing funding, training, weapons, explosives, supplies, and other material support to carry out attacks against the air domain. Also, the presence of criminal elements with extensive knowledge of the aviation sector, both within the United States and in foreign countries, pose a persistent threat to aviation and could provide potentially violent domestic groups or international terrorists with specific capabilities to exploit weaknesses in aviation security. Therefore, these three threat origins or sources cannot be viewed as being mutually exclusive, as they may combine in various forms to carry out attacks either directly against aviation assets or by exploiting elements of the air domain to prepare for or carry out attacks against the homeland or U.S. interests abroad.

---

[11] U.S. Department of Homeland Security, *The National Strategy for Aviation Security*, March 26, 2007, p. 9.

The strategy document defines three primary categories of threats against the aviation domain based on the target of the threat. These consist of: threats involving aircraft; threats to aviation infrastructure; and threats involving hostile exploitation of air cargo. A variety of tactics may be used to attack these targets, including hijackings, bombings, shootings, and criminal tactics such as smuggling of persons and weapons. A synopsis of the relationships between threat origins or sources, aviation targets, and tactics for attacking these aviation targets is presented in **Figure 1**.

Figure 1. Aviation Security Threat Sources, Tactics, and Targets



Source: CRS analysis of *The National Strategy for Aviation Security*, Department of Homeland Security, March 26, 2007.

Aircraft-related Threats. Aircraft threats may be directed at aircraft or may involve the use of aircraft to attack other targets, as was the case in the terrorist attacks of September 11, 2001. The strategy document notes that large passenger aircraft have historically been at the greatest risk from terrorist attacks, including both hijackings and bombings, because terrorists have perceived that attacks against such aircraft have significant potential to cause catastrophic damage and mass casualties and disrupt the aviation system. The document, however, notes that terrorists may also seek to attack all-cargo aircraft, especially large all-cargo aircraft which are considered attractive as weapons to attack ground-based targets in 9/11-style attacks. All-cargo aircraft, and the air cargo system in general, may also be attractive to terrorists or criminals as a means of conveyance for weapons, explosives, or other supplies. The strategy considers large transport aircraft, both passenger airliners and to a lesser extent all-cargo aircraft, to be at risk from possible attacks using shoulder-fired guided missiles or other standoff weapons.

The strategy also indicates that small aircraft face both the threat of direct attack as well as the threat that they may be used as weapons to attack ground-targets. While the strategy notes that small aircraft appear to be relatively unattractive targets

for attacks by themselves because they carry few passengers, it cautions that terrorists may use a wide variety of small aircraft, such as business jets and helicopters, to destroy ground-targets, especially critical assets and infrastructure. The most formidable threat comes from the potential use of small aircraft to either transport or deliver a WMD payload. The strategy also notes that small aircraft are also used by transnational criminal elements to carry out illegal activities, such as drugs and weapons smuggling, and pose a considerable challenge for border protection.

Finally, the strategy recognizes that non-traditional aircraft, such as unmanned aircraft, ultra-lights, and aerial-application aircraft (i.e., crop dusters), may be used as either weapons or means of conveyance for WMDs. The strategy states that terrorists may employ such aircraft for missions that are limited in range, require limited accuracy, and have a specific and small target. For example, crop dusting aircraft have been regarded as a potential threat for dispersing a chemical or biological agent. The strategy notes that such tactics deserve very close monitoring.

The strategy also briefly notes the potential threat to the air domain posed by hostile nation-states from military aircraft and missiles. However, these threats are mainly a concern for national defense and the Department of Defense (DoD), rather than a focus for homeland security, and thus have not been a major focus of the aviation security strategy and its supporting plans. This threat is, therefore, not further considered in this discussion.

Threats to Aviation Infrastructure. The strategy maintains that reported threats to aviation infrastructure, including airports and air navigation facilities are relatively few. The strategy notes that air navigation facilities, in particular, have a low public profile and are resilient to attack due to a robust multilayered design that can be quickly reconstituted thus limiting psychological and economic impacts stemming from an attack. The strategy, however, notes that there is a wide variety of potential threats to aviation infrastructure. The strategy notes in particular the potential threat to concentrations of individuals at major airport passenger terminals. Terrorists may attack passenger terminal buildings with explosives, as was attempted at Glasgow International Airport, Scotland in June 2007 and in several other historical incidents.[12]

The strategy concludes that attacks against other facets of aviation infrastructure, such as general aviation airports and air cargo handling areas, are less likely to materialize, largely because attacks against these facilities would generally not offer the opportunity to target large numbers of people and would therefore have a more limited psychological impact. The strategy, however, was released a few months before U.S. law enforcement authorities arrested members of a suspected homegrown terrorist cell who were plotting to bomb jet fuel storage tanks at New York's John F. Kennedy International Airport (JFK) and the network of jet fuel distribution pipelines in the New York City area. While the actual vulnerability of this infrastructure to such an attack remains debatable, the plot highlighted the

---

[12] See Ariel Merari, "Attacks on Civil Aviation: Trends and Lessons," in Paul Wilkinson and Brian M. Jenkins (Eds.), *Aviation Terrorism and Security*, Portland, OR: Frank Cass, 1999, for an overview of historical incidents.

possibility that aviation jet fuel storage facilities and distribution systems at major U.S. airports may be at risk. While the sophistication of this particular plot has been questioned,[13] in general, the potential threat to fuel farms and pipelines and other critical aviation infrastructure — where an attack could have a dramatic effect capturing public attention and potentially disrupting the aviation system on a large scale — may deserve further attention from policy makers and aviation security strategists.

Threats Involving Exploitation of Air Cargo. The strategy recognizes that the large scale, diversity, and complexity of the air cargo industry makes it potentially vulnerable to exploitation by terrorists. The strategy, however, concludes that post-9/11 actions to enhance air cargo security have been effective in reducing the threat of stowaways aboard air freighters that could carry out a 9/11-style suicide hijacking and the threat of explosives. Nonetheless, the strategy recognizes that the enhanced regulatory framework for air cargo security[14] is not immune to exploitation, and the air cargo system, in general, has been exploited for years by criminal elements. In addition to possible threats to all-cargo aircraft noted above, the threat of terrorist infiltration of air cargo handling operations and facilities remains a threat that could lead to exploitation of the air cargo system as a means of conveyance for terrorist operatives, and conventional weapons, WMDs, explosives, weapon components, and other terrorist items. While not discussed specifically by the strategy, it should be noted that all sorts of criminal activities, possibly including cargo-related crimes in the aviation domain, could provide revenue sources to support terrorist organizations.

Risk-Based Methodology

The U.S. National Strategy for Aviation Security is predicated on a risk-based, multi-disciplinary, and global approach to ensure that resources allocated at the federal, state, and local levels and by private sector aviation interests provide the greatest potential to detect, deter, and prevent attacks against aviation and mitigate the consequences if an attack does occur. This risk-based approach or methodology is described in detail in the National Infrastructure Protection Plan (NIPP) and the NIPP Transportation Sector Specific Plan (TSSP) which were made available to the public in May 2007.[15] In general, the NIPP serves to define the unifying structure through a common framework for identifying critical assets, conducting risk assessments, and developing and implementing risk reduction and mitigation initiatives based on the results of these assessments.[16] The TSSP applies this risk-

---

[13] See especially, Bruce Schneier, "Portrait of the Modern Terrorist as an Idiot," *Wired*, June 14, 2007.

[14] See 71 FR 30510 et seq., May 26, 2006.

[15] Department of Homeland Security, *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan As Input to the National Infrastructure Protection Plan*, May 2007: Arlington, VA.

[16] For further discussion of the NIPP and general risk management strategies for critical infrastructure protection, see CRS Report RL32561, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities,* (continued...)

based framework across the entire transportation sector, including the aviation domain.

The system-based risk-management framework outlined in the TSSP describes risk as a function of threat, vulnerability, and potential consequences, and it analyses security risk by taking into account all three of these factors. The transportation sector approach to risk management adheres to an underlying vision for risk-based decision making that seeks to establish a balance between security and freedom. The goals outlined in the TSSP include

- preventing and deterring terrorist acts against transportation systems;
- enhancing the resilience (i.e., the ability to absorb damage without catastrophic failure) of the U.S. transportation system; and
- improving the cost-effective use of resources allocated to transportation security.

The risk-based methodology seeks to achieve these three overarching goals by prioritizing resources based on risk. This approach seeks to involve extensive participation from global, state and local, and private sector entities with specific domain expertise. It also is intended to rely on inputs from the intelligence community, expert judgment, and futures analysis related to the impact or consequences of various threat scenarios.

A wide variety of risk-based transportation sector security assessment tools have been developed to assist security strategists and planners. These consist of self-assessment tools and government site evaluations, reviews, and analytic tools examining either risk as a whole, or specific risk subcomponents including threat, vulnerability, and consequence. Some specific tools being implemented to assess risk in the aviation domain include government facilitated site assistance visits and comprehensive reviews, web-based Vulnerability Identification Self Assessment Tool (VISAT) modules for airports that are currently under development, and the FAA's Information Systems Security Program (ISSP) for air traffic control systems and related functions. Communication and dissemination of this information to sector stakeholders is seen as a critical component of the risk-based strategy.

Strategic Objectives

Relying on the risk-based approach, the National Strategy for Aviation Security identifies five strategic objectives to guide aviation security activities. These include

- deterring and preventing terrorist attacks and criminal or hostile acts in the air domain;
- protecting the homeland and United States interests in the air domain;
- mitigating damage and expediting recovery if an attack against aviation occurs;

---

[16] (...continued)
and Consequences, by John Moteff.

- minimizing the impact of an attack on the aviation system and the broader U.S. economy; and
- actively engaging domestic and international partners.

According to the strategy for aviation security, terrorist attacks will be deterred and prevented by maximizing shared awareness of domestic and international airspace, aviation infrastructure, and individuals having access to the aviation system. Therefore, the strategy seeks to establish a system of protection that considers not only individual elements of the aviation system, but also their connections and interdependencies.

While the principal goals of the strategy are to deter and prevent attacks, the strategy also seeks to prepare for, and have in place, contingencies for mitigating damage and expediting recovery. The strategy identifies a need for diverse and flexible response options, for example, allowing for the selective restriction or suspension of air traffic on local or regional levels as necessary and providing decision makers with tools and resources to effectively close and reconstitute the aviation system and take other appropriate steps to prevent further attack. In general, the strategy seeks an overall approach to implementing security measures whose normal operations will minimize impacts on the flow of goods and people through the air transportation system while at the same time providing a high level of protection tailored to the unique needs of the aviation sector.

Roles and Responsibilities

The complexity and scope of the global aviation transportation systems requires cooperation among federal, state, and local government entities, international agreements and cooperation, and the participation of various industry and other private sector stakeholders to prevent, respond to, and recover from possible attacks involving aviation assets. The leading and supporting roles and responsibilities of these various entities are guided by existing laws and regulations particularly those regarding the authority to act, desired outcomes or objectives, and the availability of assets and capabilities to address aviation security needs or requirements.

At the highest levels of federal government (i.e., among cabinet-level leadership), the Secretary of Homeland Security has responsibility for coordinating national aviation security programs. In general, responsibilities of the Department of Homeland Security (DHS) include risk analysis and reviews of aviation security programs; coordination of aviation security law enforcement operations; border protection including monitoring of cross-border aviation operations and inspections and controls at all ports of entry including airports; coordinating efforts to assess and prioritize security measures for critical infrastructure and key resources (CI/KR); developing security technologies to protect against threats to aviation security such as explosives, carry-on weapons, and shoulder-fired missiles; coordination of aviation security measures and incident response; and information sharing to support and improve the global aviation security network.

Within the DHS, the TSA has the statutory responsibility for security across all modes of transportation, including aviation where it has extensive operational responsibility for passenger airline security as well as strategic planning and

regulatory responsibilities for all other aspects of security. The TSA collaborates with Department of Transportation (DOT) entities, and in particular the Federal Aviation Administration (FAA), on transportation and aviation infrastructure protection and security issues. The TSA administers a variety of programs to support aviation security, including the National Explosives Detection Canine Team program, which trains and deploys canine teams for explosives detection in aviation and other transportation modes; the Federal Flight Deck Officers Program which trains and deputizes armed pilots to defend commercial airliner flight decks from hostile actions; checkpoint and baggage screening carried out by TSA-employed Transportation Security Officers (TSOs); the use of aviation security inspectors to ensure regulatory compliance among aviation operators and related industries; Federal Air Marshals (FAMS), and the explosives operations division to respond to potential explosives threats. Additionally, the TSA maintains an intelligence function to coordinate and provide notice regarding threats to transportation, vetting passengers and aircrews, foreign students seeking flight training in the United States, airport workers, and other populations that may pose a threat to aviation or transportation security. During a national emergency, the TSA has the responsibility of coordinating transportation security-related responsibilities and activities of other departments and agencies in all modes, including aviation.

The TSA Office of Intelligence (OI) plays a central role in the transportation threat assessment process. It is the only federal entity focused solely on transportation and aviation security threat assessment. As such, it has developed a wide range of threat assessment products, based on analysis of intelligence information provided by the National Counterterrorism Center (NCTC) and other components of the intelligence community. These include a transportation intelligence gazette; comprehensive transportation-related threat assessments; annual modal threat assessments for all transportation modes including aviation; special threat assessments of specific events; weekly intelligence reports; suspicious incident reports; intelligence notes on transportation-related terrorist trends, incidents, and tactics; and transportation situational awareness notes on notable transportation-related terrorist information.

While the TSA has broad authority and responsibility for both domestic and international aviation and other transportation modes, Customs and Border Protection (CBP) has a specific primary mission of preventing terrorists and terrorist weapons from entering the United States. CBP also provides radar tracking and monitoring to support the FAA and the Department of Defense in protecting airspace around Washington, DC and throughout the continental United States. The United States Coast Guard (USCG) conducts aviation operations for national defense, law enforcement, and national security, including the specific mission of providing aerial patrols and aircraft interdiction in the National Capital Region around Washington, DC. The Department of Defense (DoD) is, however, ultimately responsible for deterring, defending against, and if necessary, defeating aviation threats within the United States and to U.S. interests globally. To meet this mission, the DoD operates as part of the North American Aerospace Defense Command (NORAD) to monitor, deter, and detect potentially hostile actions. The DoD also maintains a capability to respond to aerial threats by keeping significant numbers of fighter aircraft on alert, carrying out airborne fighter patrols over the homeland, and deploying ground-based missile defense systems around Washington, DC and other areas as warranted.

Whereas the DoD has responsibility for airborne threats, potential criminal and terror threats to aviation by individuals or groups of individuals is primarily the responsibility of the law enforcement arm of the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI). The FBI's Civil Aviation Security Program (CASP) and counterterrorism units have been involved extensively in efforts to uncover and prevent terrorist operations to attack or exploit civil aviation in the United States. The FBI has deployed over 500 airport liaison agents (ALAs) to about 450 airports with commercial passenger service to respond to aviation-related incidents and threats and participate in vulnerability assessments and planning at the airport level of analysis.

There are a myriad of other agencies and organizations that play important roles in operational aviation security. The DHS Science and Technology (S&T) Directorate maintains research and development programs to enhance aviation security, especially to address explosives threats and threats to aircraft from shoulder-fired missiles. Additionally, the multi-agency Joint Planning and Development Office (JPDO) has responsibility for designing and overseeing the implementation of the future air transportation system, including its security components. However, the degree to which the JPDO plans for future aviation security systems are integrated with DHS aviation security technology initiatives has not been fully assessed at this point.

In addition to these efforts, the Department of State has overall responsibility for outreach and coordination with foreign governments to enhance cooperation in improving aviation security. Ongoing State Department efforts includes initiatives to improve data sharing for advance passenger prescreening, and programs to reduce stockpiles of standoff weapons, including shoulder-fired missiles, which pose a threat to civil aircraft. Also, the Department of Commerce plays a role in international trade negotiations and by developing U.S. policy and regulation regarding aviation trade an security issues, while the DOT, in coordination with the Department of State, negotiates international agreements regarding airline and other commercial aviation activities. Additionally, the intelligence community, coordinated through the Office of the Director of National Intelligence (ODNI) plays an important role in assimilating and assessing intelligence — collected through signals interception (SIGINT), imagery (IMGINT), and human collection (HUMINT) — on threats exploiting aviation security measures. Additionally, other DHS components, including the Federal Emergency Management Agency (FEMA), the Domestic Nuclear Detection Office (DNDO), and the Office of Infrastructure Protection (OIP) have various responsibilities related to infrastructure protection and critical incident response in the aviation domain. Also, the Department of Energy provides scientific and technical expertise regarding nuclear weapons, radiation detection capabilities at airports to detect possible nuclear weapons or radiological materials, and coordinating response to any radiological contamination resulting from a possible nuclear or radiological attack.

In addition to the federal role, a variety of industry advisory groups have been established to provide insight and recommendations for guiding transportation security policy and practice. Most notably, the Aviation Security Advisory Committee (ASAC) exists to support the TSA by providing advice and developing

recommendations for improving aviation security methods, equipment, and procedures. The ASAC has been in existence since before September 11, 2001 and advised the FAA on aviation security matters, and has continued in this role, now supporting the TSA in its role as the lead federal agency for aviation security issues. Also, the National Research Council (NRC) and the Transportation Research Board (TRB), components of the National Academies, provide venues for information sharing and analysis of transportation security policies and practices among researchers, practitioners, and other subject matter experts. Additionally, airports, airlines, and other aviation industry stakeholders as well as state and local security and law enforcement entities play an important role in shaping and carrying out the national aviation security policy and strategy, largely by working in cooperation and coordination with the TSA to design and execute aviation mode-specific security plans.

Aviation Mode-Specific Plans

The DHS had developed a suite of aviation mode-specific plans that serve as a general framework for implementing the national strategy for aviation security under normal operating conditions, in response to an eminent threat or ongoing terrorist attack involving the aviation domain, and during recovery and reconstitution of aviation system functions and services following a potential attack.[17] Specifically, the *Aviation Transportation System Security Plan* most directly addresses the day-to-day security measures and programs to reduce the vulnerability of the air transportation system to terrorist actions or other criminal acts. This plan is augmented by the *Air Domain Surveillance and Intelligence Integration Plan* which coordinates intelligence gathering, analysis, and dissemination within the air domain. In addition, the *International Aviation Threat Reduction Plan* and the *International Outreach Plan* provide a framework for working with other nations to improve the global aviation security network with an emphasis on outreach to promote the implementation of effective security practices worldwide.

Upon recognition that a terrorist or criminal attack targeting or exploiting aviation assets was taking place, the *Aviation Operational Threat Response Plan* would be activated. This plan considers specific actions and concepts of operations for mitigating the consequences of a broad array of attack scenarios. This plan is augmented by the *Domestic Outreach Plan* which considers the involvement and coordination of state, local, and tribal government resources and private sector entities in responding to such an event, focusing most specifically on strategies for incident communications as well as the dissemination of threat information during routine operations. An *Aviation Transportation System Recovery Plan* is also being developed by the DHS to facilitate rapid recovery following a possible terrorist attack or similar disruption to the air transportation system. The goal of the recovery plan is to mitigate the operational and economic impacts of such events on the aviation system.

---

[17] The supporting plans, along with the National Strategy for Aviation Security, can be viewed at [http://www.dhs.gov/xprevprot/laws/gc_1173113497603.shtm].

Some Possible Issues for Congress

While the above discussed national policy and strategy for aviation security and the supporting mode specific plans provide an important framework for structuring aviation security measures in the United States, these documents themselves can appropriately be viewed with a critical eye to identify any potential shortcomings in underlying assumptions and approaches. In the process of congressional oversight and legislative debate, specific questions regarding aviation security policy and strategic approaches may arise. Some possible issues that may arise as the result of oversight or legislative debate may include

- the validity of underlying risk assumptions made in developing the aviation security policy, national strategy, and mode-specific plans;
- the adequacy of considerations regarding the sustainability of the aviation security system and its various components;
- whether the policy and strategy are forward-looking, or rather, do they perpetuate a reactive approach to security planning in the aviation domain;
- the extent to which the policy and strategy provide a comprehensive framework for developing and maintaining a robust aviation security system; and
- the extent to which objectives and approaches outlined in the national strategy align with budgetary processes and resource availability to ensure that strategic objectives can be adequately met.

These possible issues are discussed in further depth below.

What is the validity of underlying risk assumptions?

Determining the validity of the various risk models and assumptions that have been used to set aviation security policy and strategy is a difficult task. These risk determinations have largely arisen from restricted access intelligence information and other limited distribution sources, thus constraining the ability to engage in open public discourse on the validity of their underlying evidence and assumptions. Nonetheless, some critics have argued that these risk assumptions and resulting policy and strategic decisions may be based on inaccurate and incomplete analysis. For example, some have noted that federal intelligence and security agencies are "inexperienced with and uninterested in statistics."[18] This has led some to argue that the use of statistical techniques to study terrorism data is sorely needed, although it has been questioned whether the federal government has necessary capability and expertise to assess the reliability of available data, and use reliable methods to perform statistical analyses.[19] Instead, some have argued that "security agencies seem to advance policies without any empirical basis", relying instead on anecdotal

[18] Zack Phillips, "A Feel for Numbers," *Government Executive*, October 1, 2007, p.52.

[19] Ibid., p. 54.

evidence, political pressures, or "gut feelings."[20] Such a basis for setting policy and establishing strategies for homeland security and aviation security can result in inappropriate estimates of risk — overstating the risk of certain scenarios while underestimating the risk of others. While it appears that efforts are being made to better document global terrorism incidents and perform statistical analyses to identify risk trends, more comprehensive efforts to look specifically at risks to the aviation domain may be needed to provide better guidance for developing and refining aviation security policies and strategies. Congress may specifically examine DHS efforts to employ reliable statistical tools and techniques to validate underlying risk assumptions cited as the justification for pursuing certain courses of action to implement aviation security policies and strategies.

To what extent do the contents of U.S. policy, national strategy, and mode-specific plans for aviation security align with recommendations of the 9/11 Commission, and statutory requirements related to the implementation of those recommendations?

Congress has relied heavily on the findings and recommendations of the 9/11 Commission in setting legislative priorities. The 9/11 Commission recommendations provided a framework for consideration of legislation enacted in both in the 108th Congress when the Commission's final report was first released in 2004 (see P.L. 108-458), and during the first session of the 110th Congress in 2007 (P.L. 110-53).

With regard to aviation security, both the 9/11 Commission and subsequent legislation have emphasized policies and strategies to aggressively pursue capabilities to detect explosives on passengers, and pursue technologies to better screen passengers and carry-on items for a broad array of threat objects.[21] The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) specified that the DHS should give a high priority to checkpoint screening technologies for detecting nonmetallic, chemical, biological, radiological, and explosives and directed the DHS to develop a strategic plan for the deployment of explosives detection technologies at checkpoints, such as walk-through explosive detection portals, document scanners, shoe scanners, and backscatter x-ray scanners. The act authorized funding for the development and testing of these various checkpoint screening technologies. However, while the TSA has also recognized the importance of enhancing passenger screening capabilities, progress has been slow in developing the required checkpoint screening strategy and results of using these technologies in airport settings has been mixed, prompting Congress to include language in the Implementing the 9/11 Commission Recommendations Act of 2007 P.L. 110-53) requiring the DHS to finalize its checkpoint screening strategic plan and begin implementing it by the summer of 2008.

---

[20] Ibid., p. 54.

[21] For this and other formal recommendations of the 9/11 Commission, see National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report.*

Progress, however, has been slowed by technology hurdles including reliability issues with walkthrough explosives trace detection portals deployed for field testing and the failure of shoe explosives scanners tested on Registered Traveler program participants in Orlando, Florida to meet minimum standards set by the TSA. The TSA has also been faced with shifting technology strategies prompting them to pursue liquids explosives screening technologies as well. The TSA has reported good results in evaluations of highly sensitive handheld explosives trace detection sensors that are now being field tested for screening carry-on liquids at passenger checkpoints. While technology testing is progressing, a clear strategic picture of how these emerging technologies will be deployed to upgrade and enhance screening checkpoints is still needed. The recent mandate in P.L. 110-53 to develop and implement such a strategy appears to address this need. However, further congressional oversight of the TSA's progress in implementing the strategic plan for emerging checkpoint screening technologies may be scheduled to ensure that appropriate and effective program and budgetary decisions are made to achieve strategic goals.

The 9/11 Commission emphasized the need for the federal government to take over the role of checking passenger names to allow for thorough vetting of passengers against the comprehensive, consolidated terrorist watchlist maintained by the federal government. While this objective has largely been accomplished by Customs and Border Protection (CBP) for all inbound international flights, efforts to deploy a system for federal prescreening of passengers on all domestic flights has been repeatedly delayed amid continued controversy over privacy rights, protection of personal data, and adequate procedures for redress when individuals are falsely denied boarding or singled out for additional screening. While Congress has generally concurred with the 9/11 Commission's view that comprehensive passenger prescreening against the consolidated watchlist is needed, Congress has also been sensitive to these privacy rights, data protection, and redress concerns, and through legislation has placed specific contingencies related to these issues on system implementation, and has repeatedly directed the GAO to carefully scrutinize the TSA's progress in addressing specific requirements for full-scale system deployment. Further congressional oversight of TSA's progress toward implementing federally-run passenger prescreening on domestic flights may be called for, as the strategic plan indicates that implementation of this initiative is expected in 2008.

The 9/11 Commission also recommended that ongoing initiatives to integrate checked baggage explosives detection systems (EDS) with airport baggage handling systems should be expedited. Congress has placed an emphasis on funding airport projects to integrate EDS in-line with baggage handling conveyors, establishing the Aviation Security Capital Fund for this purpose as part of the Vision 100 - The Century of Aviation Reauthorization Act (P.L. 108-176) in 2003. Nonetheless, the GAO estimates that making the needed changes at all airports in the United States to integrate EDS equipment will not be completed until 2024 if future funding remains consistent with historic funding levels for thee activities.[22] In recognition of this

---

[22] U.S. Government Accountability Office, *TSA Has Strengthened Efforts to Plan for the Optimal Deployment of Checked Baggage Screening Systems but Funding Uncertainties* (continued...)

continuing funding need, Congress took the unusual step of including a 20-year reauthorization of funding for in-line baggage system deployment, extending authority for the Aviation Security Capital Fund and other funding mechanisms for in-line EDS integration through 2028, and directed the TSA to take further steps to prioritize airport EDS integration projects as part of the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53). Oversight of TSA strategies and plans for funding airport projects related to EDS integration may be of long-lasting interest for Congress given the size, scope, complexity, and cost of this initiative.

In addition, the 9/11 Commission recommended that the TSA intensify efforts to identify suspicious cargo, and appropriately screen and track potentially dangerous cargo in aviation as well as in maritime operations. Toward this objective, the TSA has issued regulations to increase the security of air cargo operations and has been pursuing risk-based targeting capabilities to identify shipments requiring additional scrutiny to direct physical screening resources toward elevated risk cargo with some amount of random screening. Congress, however, has been pushing the TSA toward increasing the amount of cargo destined for passenger aircraft that is screened, and in 2007 passed legislation (see P.L. 110-53, Sec. 1602) that requires the TSA to establish a system to screen 100% of cargo transported on passenger aircraft by the summer of 2010. Unlike the requirement for 100% checked baggage screening which was tied to a specific technology, namely EDS, the mandate for 100% screening of cargo placed on passenger aircraft can be met using a variety of approaches, including x-ray systems, EDS, trace detection technologies, canine teams, and possibly other methods for physical examination as approved by the TSA. To address this mandate and achieve 100% screening of cargo placed on passenger airlines within the three-year time frame set forth in the legislation, the TSA will need to move relatively swiftly in developing and implementing a strategy for cargo screening. Given the continued congressional interest on the issue of air cargo security, it is likely that extensive oversight of the TSA's progress toward meeting this mandate and effectively conducting air cargo screening operations will occur over the next few years.

While the national strategy and mode-specific plans acknowledge and emphasize passenger prescreening, checkpoint screening, in-line EDS integration, and cargo screening issues, the extent to which DHS efforts on these matters align with congressional views and legislative mandates remains a specific topic for ongoing analysis and debate.

---

[22] (...continued)
Remain, Statement of Cathleen A. Berrick, Director Homeland Security and Justice Issues, Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives, June 29, 2006, GAO-06-875T.

Does the National Strategy for Aviation Security and its supporting plans sufficiently consider the sustainability of the aviation security system and its various components?

One seemingly unavoidable reality for aviation security strategists is that continued growth in demand for air travel and for shipping goods by air is anticipated. The FAA estimates that the number of airline passengers will increase at an annual rate of about 3.4% domestically and about 4.7% for international flights over the next twelve years.[23] This anticipated growth could strain passenger and baggage screening operations in the future if it is not adequately planned for. Similarly, growth in air cargo volume is expected to increase at an average annual rate of 3.5% domestically and by 6.7% on international routes through 2020. Strategies and initiatives to enhance the security of air cargo operations and screen air cargo shipments must, therefore, also consider these growth projections in carrying out policies, strategies, and plans for enhancing air cargo security. Air traffic is also expected to increase about 3.8% with a growth of about 3.7% in general aviation operations expected. Airspace security strategies and approaches may need to consider this growth in flight operations in devising effective security programs and procedures for protecting airspace over areas considered critical for national security.

It remains unclear, however, whether this anticipated growth in aviation operations is being adequately planned for in the context of national strategies and mode-specific plans for aviation security. The strategies indicate that they will evolve with shifting threat and vulnerability characteristics on the basis of ongoing risk assessments. However, the degree to which the changing nature, size, and scope of aviation and air travel is being considered in these risk assessments remains a signficant issue for policymakers and aviation security strategists.

With regard to the sustainability of aviation security technologies, specific strategies for maintaining deployed technologies and phasing-in next generation screening technologies have not yet been clearly defined. While plans for enhancing aviation security under the comprehensive Next Generation Air Transportation System (NGATS) initiative envision extensive improvements to aviation security by 2025, the roadmap to achieving these capabilities has not yet been fully defined. According to the future concept of operations for aviation and airport security, significant security transformations will include

- integrated dynamic risk management solutions;
- biometric technologies for airport access controls;
- smaller footprint, multi-threat detection capabilities for screening passengers and baggage;
- network-enabled environmental sensors to detect and warn of chemical, biological, radiological, nuclear, and explosives (CBRNE) threats at airports;

---

[23] FAA growth estimates are based on data provided in Federal Aviation Administration, Aviation Policy and Plans, *FAA Aerospace Forecasts, Fiscal Years 2007-2020*.

- rapidly deployable, reconfigurable screening systems to meet temporary and intermittent screening requirements;
- on-board aircraft safety modifications and ground-based systems and procedures to protect flights from shoulder-fired missiles;
- network-centric information sharing capabilities for data mining and decision support to aid security operations personnel and security analysts; and
- capabilities to allow for CBRNE screening of all air cargo items not packed in secured areas or securely conveyed to aircraft.[24]

While all of these objectives are reflected to some degree in the National Strategy for Aviation Security and the supporting plans, Congress may have a particular interest in how the strategic plan aligns with NGATS plans for enhancing aviation and airport security over the next 18 to 20 years.

Is the national strategy for aviation security forward-looking, or does it perpetuate a reactive approach to strategic security planning in the aviation domain?

As previously noted, some experts have expressed concern that the DHS may be relying too heavily on "gut feelings" and anecdotal evidence in pursuing certain courses of action reflected in aviation policies, strategies, and plans. Similarly, some have questioned whether the DHS and the TSA approach to aviation security has taken on too much of a reactive stance, failing to strategically plan resource allocation based on robust and thoughtful risk analysis, instead allowing high profile events and media reaction to potentially influence decision making.

For example, using the TSA's response to the foiled liquid explosives plot in August 2006 by restricting carry-on liquids, some critics have argued that the Administration is allowing single events and the media coverage and public attention they generate to shape policy decisions.[25] The TSA has defended its actions in response to the liquid explosives threat, making available to the public documentation and demonstrations of the formidable threat posed by improvised liquid explosive devices. However, liquid explosives have long been known by security experts to pose a formidable threat to aircraft, yet U.S. aviation policy and strategy before this plot was uncovered had not included any specific near-term measures to screen passengers for liquid explosives.

Critics argue that reacting to single events is near-sighted and goes against the very purpose of developing strategies and plans in the first place, which is to be proactive in assessing threats and directing resources to mitigate associated risks. However, on the contrary, if strategies and underlying plans are to be adaptive, they should be able to shift rapidly in response to changing threat characteristics and changing threat levels. Reviewing the TSA response to the liquid explosives plot

---

[24] Joint Planning and Development Office, *Security Annex, Concept of Operations for the Next Generation Air Transportation System (Version 2.0)*, June 13, 2007.

[25] Zack Phillips, "One Hit Wonders," *Government Executive*, October 30, 2006.

may provide more specific insights into whether this response was a reasonable adaptive approach to mitigate unforseen risks or a case of taking immediate, and arguably questionable, actions in an effort to restore and maintain public confidence in aviation security. If it is determined that the TSA's actions in response to the liquid explosives plot represented a well thought out example of an evolving strategy that can respond quickly and effectively to emerging threats, then perhaps additional questions need to be asked regarding why the emerging threat of liquid explosives was not foreseen prior to widespread public disclosure of information regarding the failed liquid explosives plot in the United Kingdom. A more detailed examination of the deliberations and decision-making regarding liquid explosives, both before and after receiving knowledge of the foiled plot can perhaps provide unique insights and "lessons learned" to aid security analysts and senior policy makers in developing strategic and tactical decision making tools to improve upon the U.S. response to future emerging threat situations.

Critics argue that the government must replace its practices of responding to single threats with more systematic approaches for improving homeland security. A lingering concern is that if aviation security policies and practices, and more broadly homeland security policies and practices, remain too reactionary, terrorists may be able to exploit this approach. Terrorist may be able to trigger reactionary responses by providing misinformation about intended targets or attack methods. This may lead to haphazard allocation or reallocation of resources that could be wasteful and inefficient, and could even result in resources being moved in a manner that could make the system more vulnerable to attack. In other words, terrorists may be able to more easily exploit a reactionary approach to aviation security by using diversionary tactics that may increase vulnerabilities in other areas or aspects of the air domain.

To what extent does the national strategy for aviation security provide a comprehensive framework for conceptualizing and implementing initiatives to develop and maintain a robust aviation security system?

In 2004, the GAO issued recommendations regarding the desired characteristics of national strategies to combat terrorism.[26] The desired elements of such strategies identified by the GAO included

- a purpose, scope, and methodology;
- a definition of the problem and an assessment of the associated risk;
- an identification of the goals and supporting or subordinate objectives and activities to meet these goals, and performance measure to evaluate progress toward achieving these goals;
- an identification of resources, costs, and a risk management analysis to determine where resources and investments should be targeted;

---

[26] U.S. Government Accountability Office, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, Statement of Randall A. Yim, Director, Homeland Security and Justice Issues before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, U.S. House of Representatives, February 3, 2004, GAO-04-408T.

- a clear definition of organizational roles, responsibilities, and coordination; and
- a discussion of how a particular strategy relates to other strategies and how plans, activities, and objectives will be integrated to meet the stated goals of the various related strategies.

While the GAO used these criteria to evaluate various national security, homeland security, counterterrorism, and infrastructure protection strategies that had been developed prior to 2004, the National Strategy for Aviation Security had not been developed at that time and has not subsequently been evaluated against these desired elements. At first glance, the aviation security strategy appears to contain or address many of these desirable characteristics. Where the strategy and supporting plans may be lacking, however, is in

- fully defining the methodology for evaluating risk and carrying out the strategy;
- fully documenting associated cost estimates and resource requirements;
- providing sufficient detail regarding roles, responsibility, and coordination, particularly among non-federal entities that are expected to participate in carrying out the various mode-specific plans; and
- clearly indicating how the various components fit into the hierarchy of national security, homeland security, and counterterrorism strategies and plans and how the elements of these various plans may be integrated both within and beyond the aviation domain.

Congress may seek to carry out a more detailed review of the National Strategy for Aviation Security to specifically identify potential needs for more detail and specificity with regard to addressing these, and perhaps other, key elements of the strategy and supporting plans.

Additionally, one of the key required features of the national strategy for aviation security is that it must be adaptive. Consequently, the national strategy and its supporting plans and documents are likely to evolve over time to address changes in threats, intelligence, terrorist tactics and capabilities, as well as new security technologies and capabilities. It is also likely that the strategy and its supporting plans will sometimes need to change quickly in the face of imminent threats. Therefore, Congress may also have a particular interest in assessing the robustness of the national strategy for aviation security and the capability of the underlying aviation security system to adapt based on shifting risk dynamics.

How do the objectives and approaches set forth in the aviation security strategy and mode-specific plans align with budgetary decision-making and resource availability?

As a final consideration, Congress and the Administration may have a particular interest in assessing how the national strategy and supporting plans align with budgetary decisions and resource availability, particularly in the context of the annual budget and appropriations process. This could be a key consideration as elements of the current strategy call for some considerable expansion of the TSA's roles and responsibilities. For example, DHS objectives for the TSA to assume passenger identification functions and carry out behavioral observation both at and beyond airport screening checkpoints is likely to be human resource intensive and, therefore, may need further scrutiny in the context of budget and resource prioritization. Also, technology advancements for checkpoint, baggage, and cargo screening are also being sought by both Congress and the Administration. Additionally, new and proposed statutory requirements may also expand the functions of the TSA and other federal agencies. For example, provisions in the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53) require the swift phase-in of air cargo inspections to achieve 100% inspections of all cargo carried on passenger air carrier aircraft within three years. This mandate is likely to have significant cost and resource implications not only for the federal government, but also for the airline industry. Aligning this initiative with ongoing strategic plans for risk-based profiling and targeting of cargo shipments and investment in cargo screening technologies is likely to be a topic of considerable interest in the context of the federal budget process over the next few years.

As part of the budget process, the TSA has prepared a *Strategic Context* component of its *Congressional Justification* documents since the FY2007 budget cycle. While these documents provide a general framework of key strategic issues for the TSA, they adhere to a program level justification and analysis and do not provide in-depth discussion of how specific programs and initiatives address specific strategic issues and risk management practices. While these documents provide a general framework for understanding TSA programs in the strategic context, they may not provide sufficient detail regarding the methods used to set priorities and how the various aviation security programs and initiatives being pursued align with risk-based priorities.

As Congress proceeds with initiatives to oversee and possibly modify U.S. approaches to aviation security, substantive issues relating to the contents of aviation security policy, national strategy, and planning documents may be a considerable focus of discussion and debate. While these documents will likely play an important role as a general blueprint for guiding aviation security policy and strategy, it is also likely that the U.S. approach to aviation security will need to continually evolve and adapt to shifting threats and vulnerabilities. Addressing funding and resources to address shifts in risk and security strategy may be an issue of considerable interest in the context of future year budget planning and debate.