

National Aviation Security Policy

The National Strategy for Aviation Security, and Air Domain Awareness: A Strategic Vision

Authors:

Kathleen M. Meilahn (Booz Allen Hamilton)

Meilahn_Kathleen@bah.com or 703-412-6545

Andrew Donica (Booz Allen Hamilton)

Donica_Andrew@bah.com or 949-525-5076

Contributors:

Al MacQuoid (Booz Allen Hamilton)

Allison Wolff (Booz Allen Hamilton)

Abstract:

Aviation Security is a critical aspect of the active layered, defense in depth of our country. One aspect of Aviation Security, Air Domain Awareness (ADA), enables protection of the United States (U.S.) by providing a proactive and persistent strategic detection and prevention capability via a comprehensive understanding of the Air Domain and all entities within it, including potential threats. ADA in short consists of collection, integration and analysis of surveillance, intelligence and any-source information, and the timely sharing of this information with those who need it in order to make decisions or operate effectively. ADA is complex and requires efforts by the United States Government (USG) at all levels, and is “ best achieved by integrating public and private aviation security global activities into a coordinated effort...” (*National Strategy for Aviation Security/NSAS*, 2007, 2)

Because of the complexity, the U.S. must take a whole of government approach to address both domestic and international partnerships, interests, roles and responsibilities, ensuring all of the multifaceted aspects of Aviation Security are addressed.

Governance for the enterprise must be decided upon by the Administration. Congress must allocate funding for aviation security activities to enable the designated departments and agencies to carry out their responsibilities. Policies, procedures, and laws must be reviewed with an eye to deconfliction, and solutions. Certain laws (such as the constitutional right to *habeas corpus*) will not change, but policies and procedures may be established to ensure certain critical USG decision-makers receive information necessary to make operational decisions or to advise the President (POTUS) in a timely manner when the situation dictates, on a case-by-case basis.

Requirements across the USG must be identified (both materiel and non-materiel) and eventually consideration must be given to developing a method or process for the various agencies and departments to work together toward a combined whole of government approach to requirements solutions. An interagency capability deployment and resource allocation strategy, or multiple functionally oriented strategies, will be required to develop solutions to address those requirements in a collaborative manner.

The intelligence community and Department of Defense must work together to develop the Air Domain Intelligence and Information (ADII) aspect of ADA. ADII can be summed up as the collection, processing, analysis, production, integration and dissemination of air domain intelligence and information which includes “every source” data, including non-classified material, day-to-day information, and information that is useful to Law Enforcement, Homeland Defenders, and other Civil Security officials. ADII requirements must be identified; policy, procedures and technology issues must be addressed; and decisions must be made on how to operationalize ADII.

EXECUTIVE SUMMARY

Aviation Security is a critical aspect of the active layered, defense in depth of our country. One aspect of Aviation Security, Air Domain Awareness (ADA), enables protection of the United States (U.S.) by providing a proactive and persistent strategic detection and prevention capability via a comprehensive understanding of the Air Domain and all entities within it, including potential threats. ADA in short consists of collection, integration and analysis of surveillance, intelligence and any-source information, and the timely sharing of this information with those who need it in order to make decisions or operate effectively. ADA is complex and requires efforts by the United States Government (USG) at all levels, and is “ best achieved by integrating public and private aviation security global activities into a coordinated effort...” (*National Strategy for Aviation Security/NSAS*, 2007, 2)

Because of the complexity, the U.S. must take a whole of government approach to address both domestic and international partnerships, interests, roles and responsibilities, ensuring all of the multifaceted aspects of Aviation Security are addressed.

Governance for the enterprise must be decided upon by the Administration. Congress must allocate funding for aviation security activities to enable the designated departments and agencies to carry out their responsibilities. Policies, procedures, and laws must be reviewed with an eye to deconfliction, and solutions. Certain laws (such as the constitutional right to *habeas corpus*) will not change, but policies and procedures may be established to ensure certain critical USG decision-makers receive information necessary to make operational decisions or to advise the President (POTUS) in a timely manner when the situation dictates, on a case-by-case basis.

Requirements across the USG must be identified (both materiel and non-materiel) and eventually consideration must be given to developing a method or process for the various agencies and departments to work together toward a combined whole of government approach to requirements solutions. An interagency capability deployment and resource allocation strategy, or multiple functionally oriented strategies, will be required to develop solutions to address those requirements in a collaborative manner.

The intelligence community¹ and Department of Defense must work together to develop the Air Domain Intelligence and Information (ADII) aspect of ADA. ADII can be summed up as the collection, processing, analysis, production, integration and dissemination of air domain intelligence and information which includes “every source” data, including non-classified material, day-to-day information, and information that is useful to Law Enforcement, Homeland Defenders, and other Civil Security officials. ADII requirements must be identified; policy, procedures and technology issues must be addressed; and decisions must be made on how to operationalize ADII.

BACKGROUND

Since 1931, the first recorded attempt at aircraft hijacking by Peruvian revolutionaries, U.S. and international aviation security prevention and response procedures have been emplaced in response to acts of criminal violence and air piracy. International agreements, legislation and policies alike were mostly event-driven and responsive versus proactive and anticipatory. The international aviation community received a rude awakening on September 11, 2001 when a suicidal hijacking exploited a weakness in the U.S. civil aviation security system and terrorists seized four commercial airliners, using them in effect as missiles, destroying both World Trade Center Towers, part of the Pentagon, and killing nearly three thousand people. Aviation threats continue to challenge the international community despite a variety of policies, strategies and agreements designed to mitigate them due to challenges with information sharing and occasional failures in operational execution. As recently as December 25, 2009, Nigerian Umar Farouk Abdulmatallab attempted to blow up an airliner originating in Europe as it prepared to land in the U.S. Unfortunately this incident highlighted intelligence challenges and information sharing failures which President Obama called a “systemic failure” in aviation security and terrorist intelligence gathering, as well as operational issues such as failure to utilize available screening equipment prior to passenger boarding. This clearly raises a number of issues relevant to many agencies and departments in the USG for which solutions must be identified. In light of recent events, it is clear that the USG must once again take a hard look at ADA and reenergize national policy and strategy for aviation security. We must become proactive and anticipatory.

NATIONAL STRATEGIC GUIDANCE

In June 2006, POTUS signed the Aviation Security Policy, outlined in *National Security Presidential Directive – 47/ Homeland Security Presidential Direct 16 (NSPD-47/HSPD-16)*. It required development of the *National Strategy for Aviation Security (NSAS)* which discussed the Air Domain, and directed development of seven supporting Plans to address specific threats and challenges. Of these, the *Air Domain Surveillance and Intelligence Integration Plan (ADSII Plan)*, serves as the foundation for Air Domain Awareness (ADA) and outlines specific roles and responsibilities across the United States Government (USG) while recognizing that “maximizing Air Domain awareness will require an unprecedented level of cooperation and coordination across Federal departments and agencies as well as across Federal, State, local, tribal boundaries and with private sector and foreign partners.” (*ADSII Plan*, 2007, 5) A herder of cats, the Secretary of Homeland Security is assigned the formidable responsibility of executing the challenging and resource-consuming objective of coordinating federal programs and initiatives to integrate and synchronize them toward a harmonized operational implementation.

The *National Strategy for Countering Terrorism (NSCT)* provides guidance related to the Air Domain as part of a discussion of “domain awareness” in general.² It specifically cites countering the most dangerous groups with global reach or aspirations to acquire and use WMD, and discusses identification or interdiction of terrorist activities in the ground, air, maritime and cyber domains. Recognizing that enemies of the US will exploit global systems of commerce, transportation, communications and other sectors to

engage us asymmetrically, the *NSCT* puts forth a number of objectives to counter these activities. One specific objective is to “attain domain awareness” which is discussed as an enabler for national defense. Noting that “today’s world is sharply defined by compression of both time and distance,” it states that domain awareness enables threat identification “as early and as distant from our borders – including territories and overseas installations – as possible, to provide maximum time to determine the optimal course of action.” Furthermore, it discusses the fact that domain awareness is dependent upon “having access to detailed knowledge of our adversaries distilled through the fusion of intelligence, information, and data across all agencies” and discusses the requirement to provide this information to operating forces “afloat, aloft, and ashore, foreign and domestic” and notes that domain awareness “supports coordinated, integrated, and sustained engagement of the enemy across the full spectrum of U.S. instruments of power,” thus highlighting that domain awareness is not simply a DoD or intelligence community³ responsibility. (*NSCT*, 2003, 25)

AIR DOMAIN AWARENESS

The *NSAS* defines Air Domain 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 infrastructures.” (*NSAS*, 2007, 2) The *ADSII Plan* defines Air Domain Awareness (ADA) as “the effective understanding of threats associated with the Air Domain that could impact the security, safety, or economy of the United States.” (*ADSII Plan*, 2007, 1) This definition is threat-centric but in order to effectively utilize ADA as an enabler for aviation security, it should be viewed as including information on day-to-day operations and entities of interest (not only threats). Also, to best comply with the *NSAS* intent for the Air Domain to be global, international and include foreign airspace, and with the *NSCT* intent to mitigate potential threats as early and distant from our borders as possible, it should address entities of interest that pose a concern for potential negative impacts on interests of U.S. partners world-wide.

The *NSAS* acknowledges the fact that conventional threats remain in the Air Domain, but its focus is on countering terrorism. Concern over proliferation of WMD is noted in both the *NSAS* and the *NSCT* on a number of occasions, and the *NSAS* further addresses proliferation of MANPADS and other stand-off weapons systems, all of which are noted to be potentially utilized by terrorist groups, hostile nation-states, and criminals. Clearly such concerns indicate a necessity to somehow monitor or have access to day-to-day operational information regarding access points, transit routes, aircraft, cargo, passengers, aircrew and infrastructure in order to identify anomalies or entities of interest which have the potential of becoming a threat, so they may be addressed in a timely manner by USG decision makers and operators in order to allow for an optimal response or preventative measure.

In sum, ADA could be summarized the following way:

Air Domain Awareness is.....

- Aviation Security
- Global
- An Enabler for Decision-making and Operations
- Coalition/International
- Joint and Interagency
- All Potential Threats and Information Sources
- A Continual Process

Air Domain Awareness is NOT.....

- A DoD “Mission Area”
- Just Homeland
- Just Defense
- Just Flight Information
- Just Intelligence
- Just Surveillance
- Just Counterterrorism

To maximize Air Domain awareness, the *ADSII Plan* states that “we must transform, and integrate capabilities that collect, analyze, and disseminate surveillance, intelligence and information to create an operational picture that is tailorable to the needs of users across the United States Government, as well as at State, local, and tribal levels, and with private entities and our foreign partners.” (*ADSII Plan*, 2007, 1) Furthermore, Air Domain Intelligence and Information (ADII) is noted as having the potential to “provide the decisive element in determining adversary capabilities and intent in the Air Domain to focus policymakers and operators on the portion of that integrated surveillance picture that is most likely to contain threats, indicate the scale, kind, timing, and location of any potential attack, and inform decisions for deterring, preventing, and, if necessary, defeating attacks.” (*ADSII Plan*, 2007, 6)

In light of recent events, it is clear that the USG must once again take a hard look at ADA and reenergize national policy and strategy for aviation security. Many agencies and departments have ongoing programs and projects that enable aviation security, including efforts of the interagency Joint Planning and Development Office (JPDO) which is planning and developing the Next Generation Air Transportation System (NGATS).⁴ However, order to effectively ensure ADA, the USG must take a hard look at progress to date related to the *NSAS* and *ADSII Plan*, making decisions and taking actions to move aviation security forward in a manner that is proactive and anticipatory. The Administration should consider governance structures which may better enable ADA. Congress should consider fiscal allocations to USG agencies and departments with ADA related roles and responsibilities in order to enable them to meet their requirements. The agencies and departments themselves should discuss and review ADA requirements, and collectively develop an interagency capability deployment plan and resource allocation solution.

GOVERNANCE

As noted earlier, per the *ADSII Plan*, the Secretary of Homeland Security is assigned the formidable responsibility of executing the challenging and resource-consuming objective of coordinating federal programs and initiatives to integrate and synchronize them toward a harmonized operational implementation of ADA. However, DHS has no authority over its peer agencies and departments. It has no resourcing capability to financially enable its

peers to carry out their responsibilities. Put into analogous terms, a sibling cannot be expected to reign over her other siblings – it takes a parent to ensure all the siblings work nicely together and collaborate.⁵ The Administration should consider governance structures which may better enable ADA, versus DHS bearing the responsibility of trying to coordinate its peer agencies despite lack of authority or fiscal responsibility associated with the others.

The current aviation security policy and strategy (and associated guidance documents) are products of the previous Administration. It would be advisable for the new Administration to review current aviation security policy and strategy documents, validate them, update them, and also consider governance structures that would enable successful operationalization of ADA, thus enabling aviation security. A number of existing models could be reviewed such as that of JPDO, or of Maritime Domain Awareness (MDA), to determine the appropriate one upon which to build. It would be advisable to ensure that the National Security Staff (NSS) has oversight of aviation security via policy committee or subcommittee, monitors aviation security and ADA/ADII activities, and holds departments and agencies to task, requiring them to provide updates regarding their responsibilities and how they have executed their responsibilities.

Following governance, roles and responsibility delineation, the critical funding issue must be addressed. Congress must allocate funding for aviation security activities to enable the designated departments and agencies to carry out their responsibilities. Policies, procedures, and laws must be reviewed with an eye to deconfliction, and solutions. Certain laws (such as the constitutional right to *habeas corpus*) will not change, but policies and procedures may be established to ensure certain critical USG decision-makers receive information necessary to make operational decisions or to advise the President (POTUS) in a timely manner when the situation dictates, on a case-by-case basis. Currently, there is a problem with non-Title 50 (non-IC) entities with intelligence responsibilities being unable to access information for which they have the clearance and the clear need-to-know, but barriers exist preventing them from having information. This inhibits intelligence analysis, decision-making regarding operations and response to threats, as well as ability to advise POTUS when an event is imminent.

REQUIREMENTS DEVELOPMENT

Clearly governance must be addressed, and operational needs must be agreed upon by the USG agencies and departments with responsibilities for aviation security, before a list of requirements can be developed. These requirements will be materiel (technology and tools) and non-materiel (policy, procedures, doctrine, etc), and funding must come from congressional budgets. The challenge of resource allocation was outlined by the Government Accountability Office (GAO) in its report “Intelligence, Surveillance, and Reconnaissance: DOD Can Better Assess and Integrate ISR Capabilities and Oversee Development of Future ISR Requirements.” In this report, GAO-08-374, dated March 2008, the GAO discussed the fact that ISR integration is challenged by disparate funding across the National Intelligence Program (NIP) and Military Intelligence Program (MIP)

budgets. That being taken into consideration, imagine the complexity of allocating resources between law enforcement, civil aviation, defense and intelligence programs combined.

Again, models exist upon which a program could be built such as the DoD Joint Capabilities Integration and Development System (JCIDS) process, and the DHS Strategic Requirements Planning Process (SRPP). The afore-mentioned GAO report on ISR integration provided descriptive precedents for joint funding and staffing agreements made between agencies which worked initially but in the end were personality dependent and not obligatory, thus failed. A model must be developed which institutionalizes the requirement for USG agencies to work together to develop requirements, plan for capability deployment, and allocate resources. Perhaps multiple functionally-oriented interagency capability deployment and resource allocation strategies will be required to develop solutions to address those requirements in a collaborative manner.

AIR DOMAIN INTELLIGENCE AND INFORMATION

The intelligence community and Department of Defense must work together to develop the ADII aspect of ADA. ADII requirements must be identified, and policy, procedures and technology issues must be addressed, as well as the question of how to operationalize ADII. Clearly, effectiveness of ADII is predicated on classified activity that enables the USG to detect, deter and defeat threats as early and as distant as possible from the U.S. homeland and approaches, and U.S. interests and those of her partners abroad. Therefore, this paper will address basic concepts for policymakers to consider while addressing the problem, and will not go in depth.

Currently a number of departments and agencies address ADII. However, these efforts are challenged by such issues as lexicon, approach, or rules. Previous analytical efforts indicated a necessity to enhance the capability to further distribute or share the products these organizations create, thereby enhancing overall ADII capabilities.

Perhaps it would make sense to establish a Air Intelligence and Operations Center (AIOC) as a center of gravity for analysis and information integration, and the central clearing house for ADII products. This information should include “every source” data, including non-classified material, day-to-day information, and information that is useful to Law Enforcement, Homeland Defenders, and other Civil Security officials.

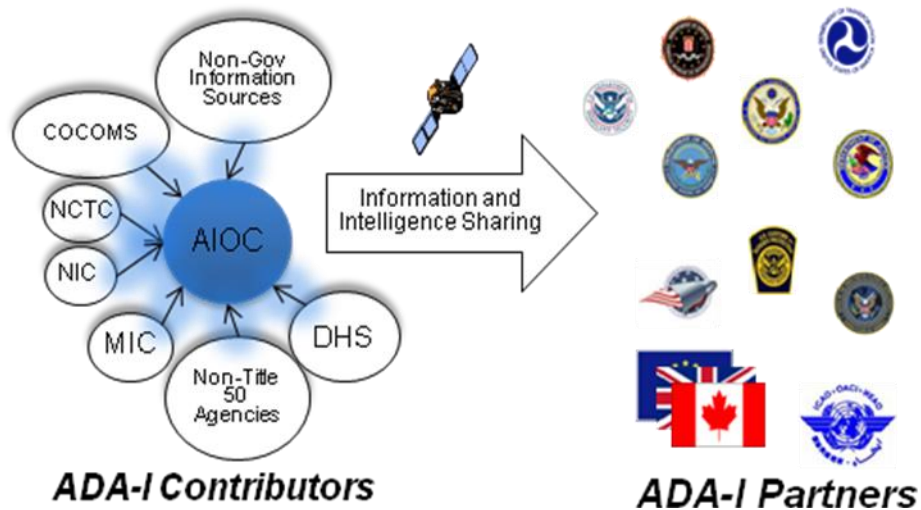


Figure 1 CAIAC Concept

Various models for an AIOC already exist and examples include: Air Combat Command’s (ACC) Air Operation Centers, Defense Intelligence Agency’s Joint Intelligence Operations Centers (JIOC), and the ODNI’s National Center for Counter Terrorism (NCTC). The graphic below (Figure 1) depicts one potential method wherein various intelligence and information sources feed the AIOC, and the AIOC becomes the central node for ADII products and information distributed to stakeholders.

SUMMARY

Recent breaches of aviation security have highlighted intelligence challenges and information sharing failures which President Obama called a “systemic failure” in aviation security and terrorist intelligence gathering, as well as operational issues such as failure to utilize available screening equipment prior to passenger boarding. This clearly raises a number of issues relevant to many agencies and departments in the USG for which solutions must be identified. In light of recent events, it would be advisable for the new Administration to review current aviation security policy and strategy documents, validate them, update them, and also consider governance structures that would enable successful operationalization of ADA, thus enabling aviation security. Congress must allocate funding for aviation security activities to enable the designated departments and agencies to carry out their responsibilities. Policies, procedures, and laws must be reviewed with an eye to deconfliction, and solutions. It is clear that the USG must once again take a hard look at ADA and reenergize national policy and strategy for aviation security. We must become proactive and anticipatory. We do not want to allow the possibility of another “9/11,” nor do we want to answer to the American people or the global community regarding our failure to prevent such a disaster, should one occur.

REFERENCES:

Air Domain Surveillance and Intelligence Integration Plan (ADSII Plan), March 26, 2007, http://www.dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf

Johnston, Nicholas and Penny, Thomas, "Obama Says U.S. Missed 'Red Flags' on Bomb Attempt (Update 1)" *Business Week*, December 30, 2009, accessed on December 31, 2009, <http://www.businessweek.com/news/2009-12-30/obama-says-u-s-missed-red-flags-on-bomb-attempt-update1-.html>

National Strategy for Aviation Security (NSAS), March 26, 2007, http://www.dhs.gov/xlibrary/assets/laws_hspd_aviation_security.pdf

National Strategy for Countering Terrorism (NSCT), February 2003, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf

¹ This is purposeful lack of capitalization in order to infer that USG departments or agencies involved in intelligence activities are not necessarily part of the Title 50 National Intelligence Community (NIC, or informally IC), which is funded by the National Intelligence Program (NIP). Per the *ADSII Plan*, the IC includes: the Office of the Director of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense involved in the collection of specialized national intelligence through reconnaissance; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of Treasury; the Office of Intelligence of the Coast Guard in the Department of Homeland Security; the intelligence elements of the Drug Enforcement Administration; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the Intelligence Community.

² In its section on Strategic Objectives on page 12, the *NSAS* notes that the *NSCT* provides overarching guidance to, and informs the *NSAS*, as does *NSPD-47/HSPD-16*.

³ This is purposeful lack of capitalization in order to infer that USG departments or agencies involved in intelligence activities are not necessarily part of the Title 50 National Intelligence Community (NIC, or informally IC), which is funded by the National Intelligence Program (NIP).

⁴ The JPDO NGATS project is as directed by the Century of Aviation Reauthorization Act and the implementation of the Intelligence Reform and Terrorism Prevention Act of 2004.

⁵ This analogy is taken from a presentation given by a member of DHS, who prefers not to be named.