NextGen Flight Security Risk Assessment Information Concept

Catherine Bolczak and Vanessa Fong
The MITRE Corporation
Center for Advanced Aviation System Development
McLean, VA

Richard Jehlen
Federal Aviation Administration
Systems Operations Planning and Procedures Office
Washington, D.C.

***Abstract*—One of the foundational elements of the Next Generation Air Transportation System (NextGen) Secure Airspace concept is the flight security risk assessment. This risk assessment is continually performed and updated based on changes to security-related information pertaining to a particular flight, as well as changes to the security environment external to the flight; e.g., other flights, airports, and airspace. This dynamic risk assessment is part of the NextGen layered, adaptive security concept in which technologies, policies, and procedures are adaptively scaled and deployed to counter a particular threat. This paper describes key information concepts for dynamic flight security risk assessment.**

Keywords-Airspace Security, Air Domain Security, Aviation Security, Flight Object, Flight Risk Assessment, Flight Risk Profile

I. Flight Risk Assessment Background

The Next Generation Air Transportation System (NextGen) Concept of Operations (CONOPS) [1] presents an integrated concept for the broad scope of Air Transportation, including Air Traffic Management (ATM), flight operators, airport management, environment, safety, weather, and aviation security. One of the major components of the aviation security concept is "Secure Airspace," whose major objective is to prevent or counter external attacks on aircraft and other airborne vehicles or use of an aircraft as a weapon to attack assets and activities on the ground. This concept has many touch points with Air Traffic Management, including the security airspaces that are established to protect ground-based assets, and flight information that is used for security monitoring and security risk assessment. Since the publication of the NextGen CONOPS and security annex [2], The MITRE Corporation's Center for Advanced Aviation System Development (CAASD) has identified candidate information to support flight risk assessment, and the potential role of the Flight Object to contain that information. This paper reflects the results of analyses performed by CAASD for the Federal Aviation Administration (FAA) in 2007-08.

This analysis has additionally been informed by the FAA's Air Domain Security Concept of Operations, signed in 2008 [3]. This document asserts the FAA's vision for its roles, responsibilities and operations for airspace security in 2025, as well as expectations for mission partners such as the Department of Homeland Security (DHS) and Department of Defense (DoD). This concept elaborates further on key elements of the NextGen CONOPS, including the flight security risk profile that will be discussed in this paper.

It is desired that this analysis be considered for global efforts to harmonize airspace security concepts and practices. Airspace security is cited as an expectation in the International Civil Aviation Organization (ICAO) Global ATM Concept [4]; also, the SESAR ATM Target Concept [5] addresses aspects of airspace security and acknowledges the need to meet security requirements and support response to unlawful acts in the air and on the ground.

A. NextGen Security Concept

"Secure Airspace" is one of seven layers in the NextGen layered, adaptive security framework at which core is the deployment of technologies, policies, and procedures in a scaled and targeted manner, in order to defeat a given threat. The layers, shown in Figure 1, provide multiple lines of defense so that security cannot be compromised via a single "breakthrough." Although the primary focus of this paper is the Secure Airspace layer, a secondary focus is the outermost layer, Integrated Risk Management. Integrated Risk Management is the ongoing process of understanding the threats, consequences and vulnerabilities that can be exploited by an adversary to determine which actions provide the greatest total risk reduction for the least impact on limited resources.

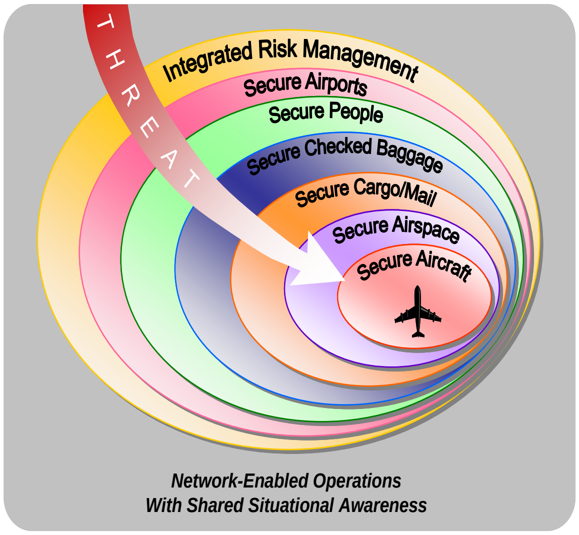


Figure 1. NextGen Layered, Adaptive Security Framework

B. *Secure Airspace Concept: Flight Risk Profile and Security Airspaces*

In the NextGen Concept, each flight will have a flight risk profile that will determine its security constraints, including constraints presented by airspaces that have restricted access for security reasons, usually to protect assets and people on the ground. Risk for flights will be continually assessed and the risk profiles will be dynamic. An initial risk profile would be created when the ATM and Aviation Security Flight Objects (to be described later) are created for each flight, when the flight's intent is initially known. In the pre-flight phase, the risk profile would be updated even as passengers are booked, screened at the airport, and baggage and cargo are screened and loaded. During active flight, the risk profile may continue to change. For example, if the destination airport has a security incident or an on-board passenger is acting suspiciously, the risk level may be elevated. The risk levels for the airspaces will also be dynamic. The interaction among the flights' risk profiles and the changing airspace restrictions in the system will continually be monitored and automatically communicated to the flight deck and security mission partners as appropriate.

Integrated Risk Management is implemented for Secure Airspace in a prevention-detection-response-recovery operational model, in alignment with the National Strategy for Aviation Security (NSAS) [1] and its supporting plans [6]. Determination of assets to be protected, procedures to be followed for flights with specified risk profiles, and responses to specific security situations are determined and re-evaluated based on a formalized risk assessment process.

II. Contributors to the Flight Risk Assessment

An important aspect of airspace security is that it is a mission shared by multiple stakeholders, both government and private sector. Each of these mission partners brings a particular perspective and roles and responsibilities driven by their individual mission areas. These perspectives, roles, and constraints drive mission partners' operational contributions to flight risk assessment and information sharing.

Beyond the organizations, there are two fundamental types of information that contribute to flight risk assessment: security-related information, and ATM-related information. The aviation security information is primarily contributed to by security, intelligence, and the flight operator. The ATM information is primarily contributed to by the Air Navigation Service Provider (ANSP) and flight operator. As depicted in Figure 2, there is some overlap and commonality of information that is relevant to both domains.

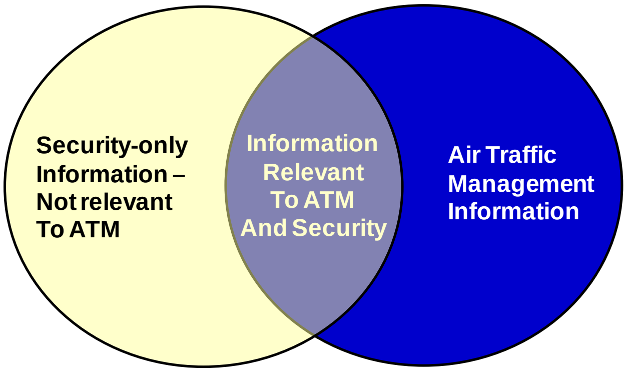

Security-only Information – Not relevant To ATM
Information Relevant To ATM And Security
Air Traffic Management Information

Figure 2. Information Contributing to Flight Risk Assessment

For NextGen, it is proposed that it is the intersection of the two that constitutes the Flight Risk Profile, which will be discussed in the next section.

III. Flight Risk Assessment Information Concept

The information concept for flight risk assessment includes five major components: Air Traffic Information, Aviation Security Information, the Aviation Security Flight Object, the ATM Flight Object, and the Flight Risk Profile. Note that in this analysis, the ATM Flight Object is described as containing only ATM-specific information. However, the ATM Flight Object will be extended to include additional security-related information that is needed for FAA to fulfill its ANSP role, including its air domain security responsibilities. Those security-related extensions have not yet been identified, but that analysis is considered a priority by the FAA to fully describe the ATM Flight Object (ATM-FO).

The overall concept for Flight Risk Assessment is described in the next several sections.

A. *Air Traffic Management Information*

As noted previously, ATM information is a major contributor to flight security risk assessment. The ANSP is in a unique position for airspace security, as the ANSP is in communication with the aircraft, can provide instructions to the aircraft, and can identify potential security anomalies in flight operations and communication. The flight operator and crew likewise contribute significant information about the flight and are aware of the status of the aircraft and on-board situation.

[1] The National Strategy for Aviation Security was published by the White House March 26, 2007.
See http://www.whitehouse.gov/homeland/aviation-security.html

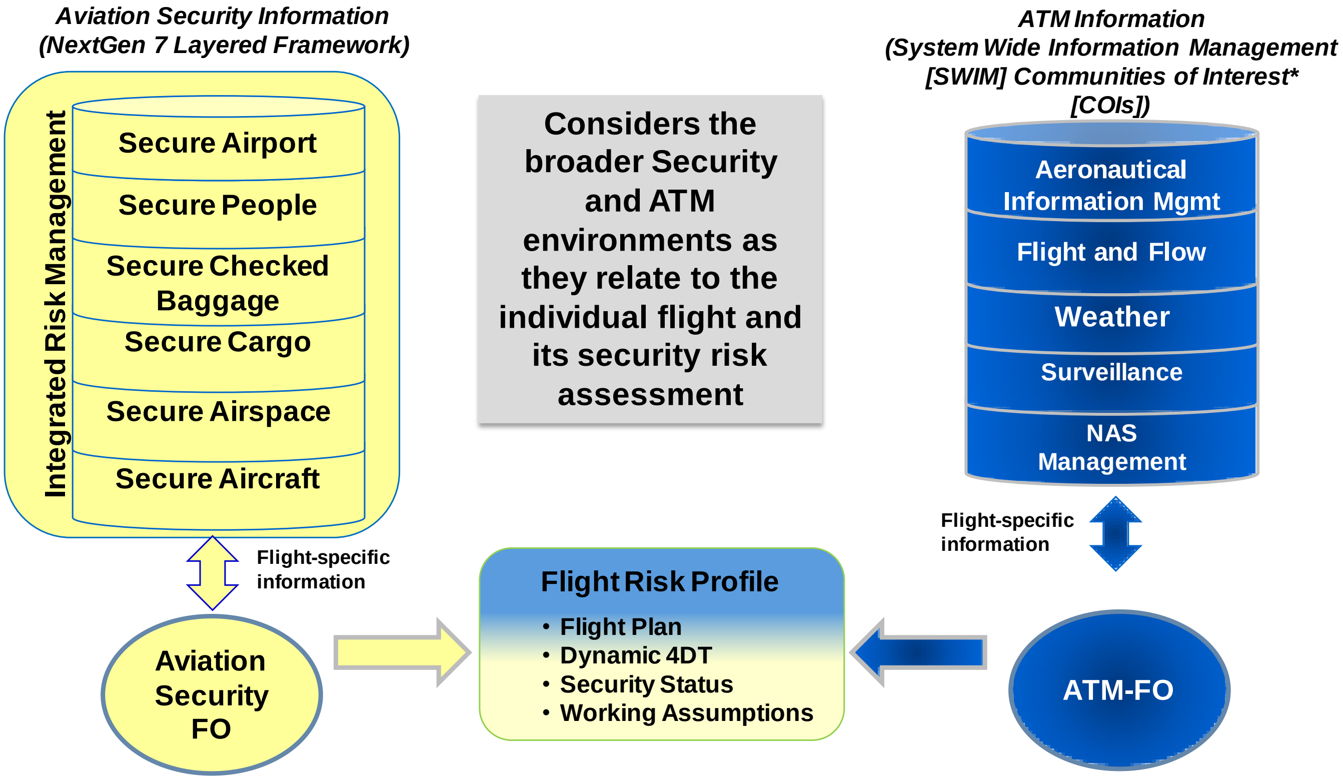
The ATM information framework is represented by Communities of Interest (COIs) identified by the FAA System Wide Information Management (SWIM) program [7]. Three of these COIs—Aeronautical Information Management, Flight and Flow, and Weather—are currently active, while the other two, Surveillance and National Airspace System (NAS) Management, have not yet been formally established. There is also potential for other NAS-focused COIs, and the Joint Planning and Development Office (JPDO) also has an activity to explore potential COIs. For purposes of this analysis, the existing known COIs were selected as representative of the types of information that describe the NextGen ATM environment, but additional work is required to fully describe the ATM information set, and is outside the scope of this analysis.

The NextGen Net-Centric Infrastructure and Shared Situational Awareness Services (SSA) provide the backbone for information access and sharing by authorized users. Users can create customized information views, such as weather constraints for a selected set of airports and flights. In this vein, the ATM-FO can be instantiated as the set of ATM environment information relevant to a particular flight.

B. *ATM Flight Object*

For purposes of this paper, the ATM-FO is considered to be that information created and controlled in the context of air traffic management, primarily by the ANSP and the flight operator. This information may be changed due to security prevention, detection, response, or recovery measures, but it is changed by people or automation performing an air traffic management or flight operation role. The ATM-FO is a flight-specific view derived from the larger scope of ATM information. This information is not changed by people or automation acting in security roles, whether they are part of the ANSP or part of a separate security provider.

Note that information views besides the ATM-FO can be created, such as linking multiple flights with specific departure airports.


Aviation Security Information
(NextGen 7 Layered Framework)
Integrated Risk Management
Secure Airport
Secure People
Secure Checked Baggage
Secure Cargo
Secure Airspace
Secure Aircraft
Considers the broader Security and ATM environments as they relate to the individual flight and its security risk assessment
ATM Information
(System Wide Information Management [SWIM] Communities of Interest* [COIs])
Aeronautical Information Mgmt
Flight and Flow
Weather
Surveillance
NAS Management
Flight-specific information
Flight-specific information
Aviation Security FO
Flight Risk Profile
• Flight Plan
• Dynamic 4DT
• Security Status
• Working Assumptions
ATM-FO

* AIM, Flight and Flow, and Weather are existing SWIM COIs. Surveillance and Infrastructure Management are potential future SWIM COIs.

Figure 3. Flight Risk Assessment Information Concept Overview

C. *Aviation Security Information*

Aviation Security Information describes all information relevant to the air domain security environment. It is based on the NextGen Layered, Adaptive security framework described earlier. To reiterate, layered, adaptive security means that procedures, policies and technologies can be deployed in a scaled and targeted manner, in order to defeat a given threat. The seven security layers are Cargo, Airport, Checked Baggage, Aircraft, People, Airspace, and Integrated Risk Management. Integrated Risk Management is portrayed as an “envelope” spanning all other layers. Each of the other layers has an Integrated Risk Management component, and there is also a unified Integrated Risk Management component that looks cross all layers. Any one or combination of the security layers can contribute to flight risk assessment; for example:

- Airport – A specific airport or set of airports (perhaps associated with a particular country or region) may be a known target for terrorism activities. Flights departing from these airports may be considered higher risk
- People – A person of interest may be on board a flight. Presence of this individual, along with knowledge of any screening performed, could be an indicator of increased security risk
- Airspace – A flight that has anomalous behavior (not in communication, not following ATC procedures) may be considered higher risk

There is a relationship between Aviation Security and ATM information. There is security-related information pertaining to ATM objects; for example, an airport can have a threat against it, a flight may have screening anomalies, and a security restricted airspace may be violated.

The NextGen SSA Services provide the backbone for information access and sharing by authorized users. Users can create customized information views, such as identifying all airports that have cargo screening anomalies or all flights that a person of interest on board. In this vein, the Security FO can be instantiated as the set of security environment information relevant to a particular flight.

D. *Aviation Security Flight Object*

Parallel to the ATM-FO, there is an Aviation Security FO, which is information created and controlled in the context of operational security, primarily by the Security Services Provider and the Flight Operator. This Aviation Security FO is derived from the overall Aviation Security information environment, which is based on the NextGen Layered, Adaptive security framework. This framework includes information related to the afore-mentioned seven security layers, each of which can have an impact on the flight risk assessment.

E. *The Flight Risk Profile*

The Flight Risk Profile is a summary of core information that is of security interest for a flight, to include both the ATM and the security perspectives. This is a characterization of the flight’s risk based on information contributed by many sources, including security providers, flight operators, ANSPs, and airport operators. While a logical construct, it can be thought of as the information viewed and manipulated by a tactical security operator. No assumptions are made as to how the information is presented to the user; however, it is envisioned that there would be a graphical flight situation display, various icons and coding schemes to indicate certain statuses, as well as tabular data fields for data entry and viewing. The Flight Risk Profile includes flight plan information, dynamic four dimensional trajectory (4DT) information, security status information, and working assumptions that drive decision-making. These components are further described in the following paragraphs. Figure 4 highlights the Flight Risk Profile, which was shown in context of the entire flight risk assessment information concept in Figure 3.

Flight Risk Profile
• Flight Plan
• Dynamic 4DT
• Security Status
• Working Assumptions

Figure 4. Flight Risk Profile

Flight Plan and 4DT. The information found in the flight plan and dynamic 4DT information provides situational awareness regarding the flight’s identity, location, capabilities, and intent. The flight plan, which is submitted by flight operators and vetted by the ANSP and security provider, contains a considerable amount of data that are relevant to flight security. For purposes of the Flight Risk Profile however, the idea is to limit the core information, and to establish links to other more detailed information. Core information includes the flight identifier, type of aircraft and route.

Dynamic 4DT information describes the flight’s current and past trajectory including current location, speed and heading, and relationship to security restricted airspaces. Note that in NextGen, it is anticipated that there will still be flight operations that are not managed by the ANSP. Currently, many flights that raise security concerns are not in communication with Air Traffic Control (ATC). In such cases, identification information is gained through visual means if possible and location is tracked through non-cooperative surveillance sources. In NextGen it is anticipated that integrated surveillance services will provide a comprehensive picture of flight locations and postulated intent. More detail on flight information related to security was provided in the FY07 analysis [8]. That analysis was performed using the ICAO flight plan as a baseline [9].

Security Status Information provides potential risk indicators, mitigations and response actions related to the flight. Notionally, Security Status Information can be expressed by a matrix, with columns represented by categories of status information, and rows represented by the aviation security layers. This information, described in the following paragraphs, includes the following:

- Flight Risk Mitigations
- Pre-Flight Risk Indicators
- In-Flight Risk Indicators
- Integrated Risk Management
- Security Response Status

Flight Risk Mitigations are information about the flight that may be viewed as reducing the level of security risk, thereby potentially moderating or obviating the need for security responses. For example, if a flight were to be out of compliance with ATC procedures, knowledge of the presence of an air marshal on board could defer raising an alert until more information can be discovered. As part of an Integrated Risk Management process, these mitigations may be applied due to flight-specific risks, or as part of a broader effort to reduce risk. Examples of mitigations include:

- Federal Flight Deck Officer presence: This indicates whether a member of the cockpit crew is trained and is carrying a firearm.
- Air Marshal presence: This indicates whether one or more air marshals are on board as a security measure.
- Airspace waivers: Flights can apply for waivers to allow operation within security restricted airspaces.
- Security capabilities: These are capabilities that the flight possesses such as cabin air monitoring, reinforced cargo containers, hardened cargo hold, and counter-Man-Portable Air Defense System (C-MANPADS) capability.

Pre-Flight Risk Indicators are attributes related to the security status of the flight prior to departure. They could impact how the flight is monitored and may generate a security response as soon as the flight's intent is made known, whether through publication of a revenue flight schedule, filing of a flight plan, generation of a departure message, or detection of a track. These attributes are frequently based on information stored in databases that are queried as soon as flight intent is known. The security response may be to deny boarding, conducting secondary screening on people or goods, restricting the flight's trajectory including possibly diverting the flight; and taking immediate response action in the event of anomalous operations. Pre-flight risk indicators do not usually change. Examples of information within this category include the following:

- Special Interest Flights [10] that originate in designated special interest countries or regions and are provided specified routing and are monitored.
- Stolen aircraft and other aircraft-related "look-out" list databases.
- Flight of interest: These are flights that are monitored due to the existence of intelligence or other adverse information that indicates they may pose a security risk. Such flights may be operated by a particular airline, or depart from a specified airport or airports within a specified country, or have a specified flight identifier, or have some combination of these and similar attributes.
- Person of interest/No-Fly on board. These flights have a person on board who is being monitored by law enforcement/security providers; when a known person of interest is boarding there are additional security measures such as secondary screening. The discovery of a No-Fly on board typically happens after the flight has departed, since this individual should not have been allowed to board, if known.
- Hazardous cargo information.

If there is a change, for example, a person of interest is discovered after the flight has left, that represents an in-flight risk (see below).

In-Flight Risk Indicators addresses the case where a flight raises a security concern while in operation. The flight may (or may not) already have pre-flight flight risk indicators; those indicators, along with security mitigations will influence the response when an in-flight risk indicator is identified. In-flight risk indicators can be raised by flight crew, flight operators, ANSP operators, or ground- or aircraft-based automation. In accordance with risk-informed security responses, thresholds exist for designating an alert based on risk mitigations and static risk indicators. Examples of operations risk indicators include the following:

- ATC non-compliance: This includes aircraft that are off flight plan, have violated security airspace (i.e., entered airspace without waivers or without following ATC procedures), or are not in communication consistent with ATC procedures. As in any ATC non-compliance situation, the ANSP will attempt to correct the problem by contacting the crew and flight operator.
- On-board problem: The flight crew, flight operator, or possibly the aircraft automation reports a disturbance [11] such as disruptive passenger, hijack, bomb threat, or mechanical or medical emergency along with change of destination request.

Integrated Risk Management integrates indicators and mitigations for the flight, and also integrates across other external security indicators. The flight itself may have a particular risk assessment based on the people and cargo on board. Externally, there may be reports of anomalous behavior or disturbances for other flights, security threats or actual attacks at airports, etc. These events may raise the overall security posture for the NAS, or may indicate increased risk specific to the flight, such as when the problem is associated with the departure airport. Examples of information in this category are discovery of new information about an on-board person of interest and a relationship to the cargo, detection of several anomalous flight operations or confirmed MANPADS attack at an airport. Integrated Risk Management can also include a quantitative risk level for a flight, which would be designated by a security services provider, such as the Department of Homeland Security. As described in [3], this quantitative risk level cues ANSP automation to re-configure security airspaces, trajectory conformance bounds, and other security responses based on pre-defined business rules. This rapid re-configuration enhances the system's ability to support layered, adaptive security operations in the NextGen aviation environment.

Security Response Status includes information pertaining to actions taken and results in response to identified in-flight risk indicators or Integrated Risk Management. This information for the most part is contributed by tactical operators in security, law enforcement, defense, and flight operator roles. Examples of information in this category include:

- Response Actions: Examples are ATC actions (communication attempts, confidence turns, rerouting, etc.), Security actions (directing law enforcement actions, researching additional security and intelligence information), Defense actions (intercepts, Combat Air Patrols [CAPs], etc.), and flight operator actions ("operations normal" confirmation).
- Results: Examples include risk mitigation information such as confirmation of secure flight deck, or risk affirmation information such as lack of response to repeated communication attempts.

Table I summarizes Security Status Information and provides several examples. Note that it is unlikely that any one flight would have more than one or two pre-flight indicators; if the flight does have several pre-flight indicators or there are several potential threats not specific to the flight, a mitigation may be to simply prevent the flight's departure. Some information may be created manually by people, while other information may be created automatically and based on thresholds. For example, if there are five simultaneous flights that are out of communication with ATC and have associated other pre-determined risk indicators, overall risk for the subject flight may be elevated. The Flight Risk Level is indicated by a discrete value; how this value would be determined and expressed, what the range of values would be, and how they would impact security responses is one of many airspace security concept research areas.

TABLE I. NOTIONAL SECURITY STATUS INFORMATION CONTENT

Risk Area	Pre-Flight Risk Indicator	Mitigation	Operations Risk Indicator	Integrated Risk Management	Security Response Status
Airport	Origin (LAX) has threat	Extra security personnel deployed	None identified	None identified	Explosives team being deployed
Cargo	None identified	Aircraft Hardened containers	Intel indicates that some cargo on board came from a suspicious shipper	Suspicious shipper has cargo on several flights from same origin airport	Investigating chain of custody
People	Person of Interest on board	Secondary Screening; FAMS	Person of interest discovered after departure	No-Fly was intercepted at origin airport for one of the same flights that contains suspicious cargo; is related to person of interest on flight	Investigating other people of interest and flights
Checked Baggage/Mail	None identified	Aircraft has hardened containers	None identified	None identified	None identified
Airspace	SIF Flight	Constrained routing provided, special ATC monitoring	Flight is not in communication with ATC	Flight Risk Level : medium	ATC attempting communication Flight Operator being contacted Working on en route
Aircraft	None identified	Counter-MANPADS capability	None identified	None identified	None identified

Working Assumptions are the final component of the Flight Risk Profile. Working assumptions are the agreed-upon suppositions or theories about threat intent upon which security operators base their decisions and actions, including determination of jurisdiction/lead agency and specific mitigation of and response to security incidents. Examples include:

- The aircraft is going to be used as a weapon
- The hijackers are holding high-value passengers hostage
- A coordinated attack is being made on airport security checkpoints

Working assumptions are not associated with specific security layers but are a summation of the security situation that is being presented to decision-makers.

A very simple example of a Flight Risk Profile's content is provided in Figure 5.

Flight ID: ABC123
Beacon Code: 4234
AC Type: B757
Route: LAX….ORD
Position: LAX VORTAC 290 40 mi
Speed: 250 kt
10 minutes to SRA

LAX security alert
Two FAMS on board
Person of Interest on board
No screening issues
Requested COD

Assume no hostile intent

Figure 5. Example Flight Risk Profile Content

To summarize, the Flight Risk Assessment Information concept has ATM and Aviation Security information repositories that represent the sets of information describing those two environments. The Aviation Security Information Repository is based on the NextGen Layered, Adaptive Security framework as presented in the NextGen CONOPS. The ATM Information repository's framework is based on the SWIM COIs. The ATM Flight Object derives from and contributes to flight-specific ATM information, and the Aviation Security Flight Object derives from and contributes to flight-specific Aviation Security information. The Flight Risk Profile logically combines core information from both the Aviation Security and ATM flight objects.

IV. Summary and Conclusions

An initial flight risk assessment information concept has been developed as an extension to NextGen Secure Airspace concept. The concept reflects that information is contributed from both ATM and aviation security perspectives. It also reflects that an individual flight's security risk profile is dependent upon both information specific to the flight, as well as information related to other flights and the overall operational security environment. To support the future vision of security Integrated Risk Management, the flight risk profiles and associated prevention-detection-response-recovery measures must be dynamically updated and applied. This dynamism, as well as the diversity of missions for airspace security stakeholders, presents significant challenges for achieving the concepts. Net-Centric Operations, including the governance mechanisms of a COI to facilitate information exchange, and architectural design to implement the data exchange, is a key enabler for the Secure Airspace concept.

As has been noted, this is an initial information concept and it requires socialization and validation with the many airspace security stakeholders. Also, potential implementation of this concept through existing and planned capabilities, whether those capabilities are organization-specific or multi-agency, needs to be evaluated. Implementation needs to be in an architecture that will support the envisioned operations to enable agility and timely information sharing.

Disclaimer Notice

The contents of this material reflect the views of the authors. Neither the FAA nor the Department of Transportation makes any warranty or guarantee, or promise, expressed or implied, concerning the content or accuracy of the views expressed herein. Approved for Public Release; Distribution Unlimited 09-0090. ©2009 The MITRE Corporation. All rights reserved.

References

[1] Joint Planning and Development Office, "Concept of operations for the next generation air transportation system," Version 2.0, Washington, DC, 2007. http://www.jpdo.gov/library/NextGen_v2.0.pdf

[2] Joint Planning and Development Office, Security Annex, "Concept of operations for the next generation air transportation system," Version 2.0, Washington, DC, 2007. http://www.jpdo.gov/library/NextGen_Security_Annex_v2.0.pdf

[3] Federal Aviation Administration, "Air Traffic Organization Air Domain Security Concept of Operations," Washington, DC, 2008.

[4] International Civil Aviation Organization, "ICAO Global ATM Concept," First Edition, Doc 9854 AN/458, 2005

[5] Single European Sky ATM Research (SESAR) Consortium, "ATM Target Concept," Toulouse, 2007. http://www.sesar-consortium.aero/deliv3.php

[6] Department of Homeland Security, "National strategy for aviation security supporting plans," Washington, DC, 2007. http://www.dhs.gov/xprevprot/laws/gc_1173113497603.shtm

[7] A. Usmani, "SWIM segment 1 details and community of interest processes," Federal Aviation Administration, 18 September 2007. http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/swim/documentation/media/briefings/SWIM%20Segment%201%20Overview%20presented%20Sept%202007%20for%20RTCA%20Annual%20Forum.ppt

[8] C.N Bolczak and C.V Fong, "Role of the flight object and 4DT in airspace security," Digital Avionics Systems Conference, DASC '07. IEEE/AIAA 26th , pp.4.E.1-1-4.E.1-11, 2007. http://www.ieeexplore.ieee.org/iel5/4391810/4391811/04391919.pdf?isnumber=4391811&prod=STD&arnumber=4391919&arnumber=4391919&arSt=4.E.1-1&ared=4.E.1-11&arAuthor=Bolczak%2C+C.N.%3B+Chih-Chia+Vanessa+Fong

[9] International Civil Aviation Organization, "Procedures for air navigation services," Air Traffic Management, DOC 4444, ATM/501, Appendix 2, Montreal, 2001.

[10] Federal Aviation Administration, "Special operations," Chapter 12, Special Military Flights and Operations, Section 14, SIFs, FAA JO 7510.4.

[11] FAA Advisory Circular 90-103, "Reporting of threats in accordance with the common strategy," 2006.

Author Biographies

Catherine Bolczak is a Principal Information Systems Engineer with The MITRE Corporation's Center for Advanced Aviation System Development (CAASD). Ms. Bolczak is currently developing airspace security concepts, requirements, and evolution plans for the Federal Aviation Administration (FAA) and Joint Planning and Development Office (JPDO), including the integration of airspace security with Air Traffic Management, air defense, and homeland security operations. Her other ATM system engineering experience includes the Next Generation Air Transportation System (NextGen), En Route Automation Modernization (ERAM), Traffic Flow Management (TFM) Modernization, System Wide Information Management (SWIM), and National

Airspace System (NAS) information architecture. She holds master's degrees in Computer Information Systems and in Computer Science from Boston University and Marymount University, respectively.

Vanessa Fong is the Director for Joint Agency Transportation Security at the MITRE Corporation's Center for Advanced Aviation System Development (CAASD). She is responsible for CAASD's Transportation Security mission area focusing on integration, situational awareness, collaboration, net-centric operations, and interoperability in shared transportation security missions across government agencies, such as the Federal Aviation Administration, Department of Defense, Department of Homeland Security, and the Joint Planning and Development Office. Additionally, she serves on the MITRE Engineering Advisory Council to enhance corporate knowledge management in systems engineering. Ms. Fong was the first director for the National Airspace System (NAS) Enterprise Architecture Council, which was created in 2004 to apply engineering and integrated domain expertise to CAASD's NAS effort. She has contributed to air traffic management projects, overseen the air traffic management laboratory and prototyping efforts, and led the development and technology transfer of the User Request Evaluation Tool. She has a master's in chemistry from the University of Wisconsin in Milwaukee; a master's in computer science from Johns Hopkins University, Baltimore, Maryland; and a bachelor's in chemistry from the National Tsing-Hua University in Taiwan. She has been named an Outstanding Woman Engineer of Color by the U.S. Black and Hispanic Engineer and Information Technology magazine.

Richard Jehlen is currently the Director of the Planning & Procedures Office in the Air Traffic Organization's System Operations Services and also serves as the Air Traffic Procedures Advisory Committee (ATPAC) Executive Director. Mr. Jehlen holds a Bachelor of Science degree from Excelsior College and has over 30 years Air Traffic Management experience. His operational experience, both FAA and Department of Defense, includes positions in the Tower, Approach Control and Air Route Traffic Control Center. During his career, his responsibilities have included: Automation, Airspace & Procedures, Traffic Flow Management, Future Concepts, Validation and Integration, Operational Planning and Requirements. Mr. Jehlen has also served as the United States' representative to ICAO (Panel/Study Group) and currently is the U.S. Panel Member to the ICAO Air Traffic Management Requirements and Performance Panel (ATMRPP).