Civil Aviation Infrastructure: Protecting A System-of-Systems
Brian M. Legan, Vice President
Christopher Kelly, Senior Vice President
Booz Allen Hamilton, Inc.

Introduction

Homeland Security Presidential Directive (HSPD)–7 designates the air traffic control (ATC) system as part of the nation’s critical infrastructure due to the important role civil aviation plays in commerce and the safety and mobility of people. This designation requires the Secretary of Transportation and the Federal Aviation Administration (FAA) to ensure that the ATC system and related systems are protected from both physical and cyber security threats to prevent disruptions in air travel.

The “Bricks and Bytes” of Our Aviation Infrastructure

An appreciation of the enormity and complexity of our U.S. National Airspace System (NAS) is essential to fully grasp the challenge of protecting critical aviation infrastructure. The NAS is the largest and safest in the world, accommodating an average of 60,000 flights per day (or over 35% of air traffic worldwide) and over 750 million passengers each year. The unparalleled aviation safety record in the United States is dependent upon a massive, distributed array of critical infrastructure components: over 600 air traffic control facilities, 450 commercial airports, 19,000 airfields, and over 64,000 communication, navigation, surveillance, and automation components and related infrastructure. This array of facilities, systems, and equipment ultimately enables people — over 15,000 air traffic controllers, 6,000 technicians, and 5,000 aviation safety inspectors — to safely and effectively manage an air traffic system that contributes over $1 trillion annually to the national economy.

In addition to this physical infrastructure (the “bricks”), the Next Generation Air Transportation System (NextGen) will rely upon an information architecture that spans the entire enterprise, employing network-centric “cloud” capabilities and the digital exchange of mission critical information (the “bytes”) provided by space-based and aircraft-based sources. The FAA’s NextGen Implementation Plan illustrates that success hinges upon building an integrated system-of-systems composed of advanced Communication / Navigation / Surveillance (CNS) infrastructure, automation, and avionics capabilities and a concurrent evolution in policy, airspace design, and workforce competencies. The migration from ground-based navigation and surveillance to space-based and aircraft-based systems is already in progress, including a phase out of some legacy systems and a phase-in of new capabilities. The FAA is increasingly reliant upon commercial satellite systems to provide essential services including communication, navigation, remote sensing, imaging, weather and meteorological support. For example, systems such as Automatic Dependent Surveillance Broadcast (ADS-B) provide more precise position, navigation, and timing information to allow pilots and controllers to enable efficient arrivals and departures from airports and preferred trajectories en route. ADS-B uses Global Positioning System (GPS) information to

---

1 FAA Administrator’s Fact Book, June 2012.
2 Ibid.
provide continual broadcast of aircraft position, identity, velocity and other information over unencrypted data links to generate a precise air picture for air traffic management. The FAA is also developing a Data Communications (DataComm) system that distributes information using commercial air-to-ground digital data link networks to connect FAA air traffic control (ATC) sites and DataComm-equipped aircraft.

As traffic volume and complexity increase, system wide information management (SWIM) will also be critical to the continued safety and efficiency of air traffic management. There is an increasing use of commercial software, Internet Protocol (IP) technologies, and web-based applications to assimilate and distribute information from a variety of sources to support ATC services. Common IT communication protocols and commercial-of-the-shelf (COTS) equipment are also being used on newer aircraft at unprecedented levels. This evolving service-oriented architecture will eventually migrate aeronautical information to a digital, cloud environment. Both aircraft and air traffic control systems will serve as “nodes” in a vast network of federated systems, supported by a range of standards-compliant and interoperable applications, running on a variety of platforms.4

Challenges and Opportunities

The implementation of the NAS enterprise architecture, network-centric ATC operations, and SWIM improves resilience and adds flexibility for continuity of operations. This evolving system architecture, for example, provides increased agility for mitigating planned and unplanned disruptions by allowing the seamless transition of information and operations to alternate sources and locations. Conversely, as our aviation network increasingly relies upon the digital exchange and sharing of information among diverse constituents (e.g., air traffic control, pilots, DoD, DHS, international airlines, third-party consumers) using various devices and applications, we become susceptible to new threats. These emerging threats may be from malicious actions, unintended interactions, or natural events. The migration from legacy, stove-piped ATC systems to an interconnected system-of-systems brings new challenges and considerations for critical infrastructure protection.

To date, critical infrastructure protection efforts and investments have been largely focused on protecting physical aviation assets. For example, passenger and baggage screening, explosive detection, video surveillance, biometrics and identity verification measures, facility access control systems, and related efforts have been the subject of intense development and debate since the formation of the Department of Homeland Security (DHS) and Transportation Security Administration (TSA) a decade ago. While these physical infrastructure protection measures are logical imperatives, they do not address the coincident and growing threats to our aviation system’s critical cyber infrastructure. We must recognize that our air transportation system is not immune to similar disruptions that have already been seen in the banking, financial, and healthcare industries.

---

Evolving Nature of Vulnerabilities and Threats

Gen. Keith B. Alexander, head of the National Security Agency (NSA) and the United States Cyber Command, cited a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011. He also acknowledged an increase in foreign cyber attacks on the United States aimed at critical infrastructure and rated our preparedness to defend against a major attack as a “3” on a scale of “1” (unprepared) to “10” (fully prepared).  

There have been several reports published recently that highlight the vulnerability of our evolving air transportation cyber infrastructure. The USDOT Inspector General audited 70 FAA web-based applications including systems that disseminate information over the Internet, such as communications frequencies for pilots and controllers, plus other internal applications used to support ATC systems. The results of these tests revealed over 3,800 vulnerabilities – including more than 750 high-risk vulnerabilities that could provide an attacker with immediate access into a computer system and allow remote execution of commands. A follow up report indicated that while FAA has taken steps to install some advanced systems in ATC facilities to detect cyber threats, most sites have still not been upgraded. In addition, a U.S. General Accounting Office (GAO) report lists several incidents where satellite services have been disrupted or denied as a result of system vulnerabilities. The DoD and GAO cite several types of threats to critical satellite-based systems including ground-based, space-based, and interference-oriented threats. FAA operational requirements necessitate the use of unencrypted ADS-B data links, which the agency believes have a low likelihood of malicious exploitation. However, research conducted by the United States Air Force’s Institute of Technology concluded that ADS-B’s unencrypted signals are susceptible to interception, jamming, and spoofing that could result in loss of situation awareness, service disruption, and potentially crashes. A recent report on Global Navigation Satellite System (GNSS) jamming discusses the susceptibility of the signals to radio frequency interference (RFI) due to: a) malicious interference, b) uninformed interference (i.e., intentional transmission of signals without intent to cause harm), and c) accidental interference from unintentional signal transmissions. Most occurrences have involved uninformed and accidental interference. This report cites recent incidents at Newark Airport and a Leesburg, Virginia site where truck drivers using personal privacy devices (PPDs) to

block position tracking by employers have caused unintentional interference with signals from both ground-based and space based GPS augmentation systems\textsuperscript{11}. In a more publicized incident, the FCC denied Light Squared’s venture to deploy an expanded wireless broadband network because it used adjacent radio spectrum that increased the probability for unintended interference with the Global Positioning System (GPS) signals\textsuperscript{12}.

These examples highlight the intersections between the objectives of government and industry stakeholders, and between public and private users of cyber infrastructure. While these cases illustrate the potential threats and challenges, they also represent opportunities to resolve these vulnerabilities and improve the overall resilience of our air transportation infrastructure. The evolution of policies, procedures, certifications and standards often lags technology development and implementation, but are essential to resolve conflicting interests and concomitant vulnerabilities. Finally, these instances underscore the need to address the vulnerabilities of: a) the physical sources of information (e.g., satellites, systems, sensors), and b) the cyber infrastructure (e.g., data links, information systems, network and processing mechanisms, cloud-based applications) that represent the NAS enterprise architecture.

**Seven Steps Toward Improved Risk Management and Resilience**

1. **Recognize that it takes a network to defend a network.** Protecting a system-of systems such as our air transportation infrastructure involves far more than having the right technology. It also involves people, policies, and analytics to proactively detect threats and counter them before consequential events occur.

2. **Develop a Cyber Security Enterprise Architecture** (Cyber EA) as an integral layer of the NAS enterprise architecture. Building in protection and resiliency at the enterprise level (versus just at the individual system level) is imperative if we are to effectively and economically thwart threats to aviation safety and security. The Cyber EA must include provisions for certifications, policies and standards, and appropriate enforcement mechanisms such as authentication, inspection, classmarks, and proxies. The Cyber EA would establish the blueprint for a scalable, enterprise-level security framework. This framework would enable future capabilities to be implemented that employ enterprise security controls, not just isolated system-specific provisions. We must move beyond “check-the-box” compliance to flexible models that adjust to the changing technological and operational environments.

3. **Improve systems integration testing** to ensure that the incremental evolution of the NextGen system-of-systems remains secure as new capabilities are introduced. The increased use of open systems architectures, COTS products and equipment, etc. may inadvertently introduce new vulnerabilities. Security requirements and specifications can be developed for customized vendor products and solutions. However, it is

---
\textsuperscript{11} Pullen, Sam. Ibid.
only through enterprise systems integration testing and independent verification and validation (IV&V) that emergent vulnerabilities can be identified and resolved prior to operational deployment.

4. **Establish a unity-of-effort to implement a dynamic defense posture.** Evolving threats can change on a daily and even hourly basis. The FAA and other government and industry stakeholders can create cyber resilience by recognizing that cyber security is not just about technology, but also about people – because they are so critical to an organization’s ability to protect itself. Considering the diverse stakeholders and objectives at play, we need a unity-of-effort to develop effective policies, standards, certifications, and engineering solutions that are acceptable by public and private stakeholders with divergent objectives.

5. **Create cyber resilience in addition to cyber defenses.** Cyber resilience is the ability to operate in the face of persistent attacks. Traditional cyber defense strategies, such as firewalls and intrusion-detection systems, are no longer enough. Cyber attacks on our critical infrastructures – including our air transportation system – are becoming so numerous and sophisticated that some inevitably get through. Resilience enables the FAA Air Traffic Organization to continue to provide service to the public and industry customers while fending off or reacting to cyber attacks.

6. **Develop and deploy sophisticated cyber analytic tools** to connect the dots across the massive amounts of flight data, CNS information, and mission support data. The network-centric ATC systems architecture creates an opportunity to apply “cloud analytics” to process dynamic data from distributed sources and identify the trends, anomalies, and relationships that lead to proactive threat detection.

7. **Implement advanced Cyber Training to educate the next generation of cyber professionals** on the latest tools, tactics, and techniques, so that they can implement solutions that meet future cyber threats and challenges head-on. Effective cyber training requires a holistic approach that involves people, processes, and technology. Threats are dynamic and evolving. Therefore, cyber training must be an integral part of an organization’s continuous improvement process rather than just a one-time exercise to earn a certificate, accreditation, or other recognition.