The Connectivity Challenge: Protecting Critical Assets in a Networked World

A Framework for Aviation Cybersecurity

An AIAA Decision Paper

August 2013

Framework for Aviation Cybersecurity

Framework for Aviation Cybersecurity

“America must also face the rapidly growing threat from cyber-attacks . . .
our enemies are also seeking the ability to sabotage our power grid,
our financial institutions, our air traffic control systems.
We cannot look back years from now and wonder why we did nothing
in the face of real threats to our security and our economy.”

– President Barack Obama, 2013 State of the Union Address

Framework for Aviation Cybersecurity

Table of Contents

Framework for Aviation Cybersecurity

Executive Summary

As a key foundation of international trade, tourism, and investment, aviation is crucial to the global economy. This reliable, safe, and efficient transportation network carries over 2.6 billion passengers a year and 48 million tons of freight. Aviation's global economic impact (direct, indirect, induced, and tourism catalytic) is estimated at $2.2 trillion or 3.5% of global gross domestic product (GDP). Disruption to this flow can result in significant economic and social disruption that would ripple across the globe, as demonstrated in the aftermath to the attacks of September 11, 2001. We now remain vigilant to adversaries who seek to disrupt the global economy by attacking aviation's critical infrastructure.

Currently, a growing threat to the safety and security of the global aviation system lies in cyberspace. Today's cyber threat actors are focused on malicious intent, the theft of information, profit, "hactivist" political motivations, and include nation states and those who act on their behalf. Adversaries are numerous, adaptive, and far-reaching. They attack continuously from multiple fronts, have multiple objectives, and work in anonymity.

As one of the most complex and integrated systems of information and communications technology (ICT) in the world, the global aviation system is a potential target for a large-scale cyber attack. With the continual and rapid integration of new technologies, the aviation industry keeps expanding, changing, and becoming increasingly connected. As technologies rapidly evolve, however, so do our adversaries and their threats. Without the appropriate cybersecurity measures in place for this evolving threat, the industry may be at risk. Therefore, it is imperative that the industry maintain the highest levels of confidence in aviation.

Currently, there is no common vision, or common strategy, goals, standards, implementation models, or international policies defining cybersecurity for commercial aviation.[1] Ensuring a secured aviation system and staying ahead of evolving cyber threats is a shared responsibility, involving governments, airlines, airports, and manufacturers. It is critical that all of these members adopt a collaborative, risk-informed decision-making model to set goals and define a cybersecurity framework and roadmap to strengthen the aviation system's resilience against attacks. This roadmap must be driven by a common vision and strategy, differentiate economic from safety-related concerns, and address all security layers including know, prevention, detect, respond, and recover. The industry must also look to examples of successful collaborative government/industry teams as a template for designing aviation cyberspace security solutions, such as the Commercial Aviation Safety Team (CAST) that developed a risk management model to reduce commercial aviation fatalities and initiated new government and industry safety initiatives.

Significant work has been accomplished in cybersecurity. The National Institute of Standards and Technology (NIST), the Federal Information Processing Standards (FIPS), the International Organization for Standardization (ISO), and the Information Systems Audit and the Control Association (ISACA) Control OBjectives for Information and related Technology (COBIT) have developed standards that provide the industry with best practices. Security working groups such as the Computer Security Incident Response Team (CSIRT) and the Computer Emergency Response Team (CERT) have functioned for nearly two decades to response to breaches of security. Major efforts in both research and education are underway at organizations such as the Center for Education and Research in Information Assurance and Security (CERIAS). This experience and knowledge can be leveraged, extended, and applied across the aviation community.

The following framework has been drafted to address the expansive topic of cybersecurity for aviation:

- **Establish common cyber standards for aviation systems:** Organizations such as NIST, ISO, and others are working with critical infrastructure providers to develop information security and cyber protection standards for critical infrastructure. Constructive participation in these activities is important to ensuring that aviation's unique requirements are considered when developing the standards.

[1] *Cyber Security in Civil Aviation*, Centre for the Protection of National Infrastructure, August 2012, p. 2.

Framework for Aviation Cybersecurity

- **Ensure a cybersecurity culture:** The same discipline that achieved aviation's high safety standard must also be applied to developing a common vision, common strategy, goals, and definitions, and a common framework and roadmap for addressing the evolving threats.
- **Understand the threat:** The aviation community must have a common understanding of the actors and their motivations and intents to efficiently plan our defenses. Our adversaries are thinking outside the box to plan cyber attacks and we must do the same to stop them.
- **Understand the risk:** To manage cyber risk, it is imperative that the industry ***identify the elements*** of the aviation system that need to be protected. The aviation system is a large and complex international entity with multitudes of stakeholders. It will take time and a disciplined process to understand the interactions of the system.
- **Communicate the threats and assure situational awareness:** It is important that government and industry share threat and mitigation data to increase the speed at which threats are mitigated across the aviation system. The Critical Infrastructure Partnership Advisory Council (CIPAC) is an existing means for U.S. government and industry stakeholders to address sensitive aviation security issues. Aviation cyber threats are also global in nature with international ramifications. Therefore, there must be mechanisms in place to exchange data with the international aviation community.
- **Provide incident response:** The aviation community must also understand the ***timeliness required for responding to threats*****.** Different events dictate different response times. For example, a change to a ticketing system may happen quickly as a software patch, whereas a change to aircraft software requires significantly more testing, certification, and approvals. Consideration must be given to these constraints within the response framework. Timely processes, methods, and standards for responding to an attack must differentiate the needs of each aviation subsystem.
- **Strengthen the defensive system:** The industry must also ***protect the elements*** of the aviation system with systems and standards. This requires protecting the interfaces between major subsystems as well as the subsystem.
- **Define design principles:** The design principles underlying the development of the Internet create opportunities for adversaries. As the cyber domain continues to grow, aviation must define design principles for its networks and control systems that consider the evolving cybersecurity threat and ensure no silent failures. This would include identifying architectures and design principles that protect critical systems and platforms against known attack methods and to ensure that aviation systems are secure by default and are resilient against unknown threat scenarios.
- **Define operational principles:** These principles focus on the operational aspects of systems deployed in the field. This would include a strong cyber culture, operational standards and best practices that mitigate threats to our systems and platforms to ensure resiliency.
- **Conduct necessary research and development:** The aviation community must focus its resources on researching and developing appropriate design and operational principles, such as: (1) creating secure and resilient system architectures, including methods for maintaining secure data transfer, isolating critical data, and effectively recovering from attacks: (2) improving attack detection; and (3) ensuring forensic readiness.
- **Ensure that government and industry work together:** Establish a government and industry framework to coordinate national aviation cybersecurity strategies, policies, and plans. This would include: (1) establishing policy for near and long term cybersecurity development; (2) defining accepted international rules of behavior; (3) enforcing consequences for bad behavior; and (4) positioning cybersecurity as a high priority on the diplomatic agenda.

Summary
Today, commercial jets span the globe with unprecedented safety and reliability. The same discipline that maintains this remarkable safety record must also be applied to better safeguard systems across the spectrum of aviation operations. As a result, it is critical that the global aviation community: (1) implement a common cybersecurity framework and implementation model to address evolving threats; (2) increase cooperation and focus within the aviation community, with the active participation of major industry players; (3) leverage, extend, and apply the existing industry best practices, response team, and research and education efforts under way; (4) bring the appropriate government agencies into the discussion; (5) begin building a roadmap by identifying near-, mid-, and long-term actions; and (6) establish a governmental and

industrial collaborative framework to coordinate national aviation cybersecurity strategies, policies, and plans.

1) Introduction

The global aviation system is at a crossroads. The aviation industry is expanding, changing, and becoming increasingly connected. Due to the rapid rate of innovative technologies entering the aviation marketplace, connectivity is increasing at an exponential rate. The aviation industry is now dependent on information and communications technology (ICT) to operate the global air transportation system.

Introducing new technologies without robust cybersecurity measures in place presents a risk to the industry, in light of evolving cyber threats. Aviation is renowned for being one of the safest modes of transportation, and safety is paramount. For this reason, all aviation industry stakeholders must fully understand the risks to their networks and control systems from cyber threats and take steps to close the gaps and potential vulnerabilities to maintain public confidence in the aviation system.

The global aviation system includes distributed networks, varied organizational structures and operating models, and interdependent physical and cyberspace functions and systems, as well as governance constructs that involve multi-level authorities, responsibilities, and regulations. Recent government actions, like the issuance of U.S. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience,* highlight the risk to critical infrastructure.

Today's cyber threat actors are focused on malicious intent, the theft of information, profit, and to some extent, "hactivist" motivations of furthering political goals. Adversaries are numerous, adaptive, and far-reaching. They attack continuously from multiple fronts, have multiple objectives, and work in anonymity. In addition to external adversaries, we must protect against insider attacks both from intentional and unintentional actors. It is not a question of *if* there will be an attack, but rather *when*, and what the outcome will be.

Currently, there is no common set of standards or international policy defining cybersecurity in commercial aviation.[2] This document outlines a framework for helping the aviation community build a roadmap for ensuring that aviation's critical infrastructure is secure and able to withstand and rapidly recover from the evolving threats. This framework addresses all security levels including know, prevent, detect, respond, and recover.

Aviation's contribution to the world economy

As a key foundation of international trade, tourism, and investment, aviation is crucial to the global economy. This reliable, safe, and efficient transportation network carries over 2.6 billion passengers a year and 48 million tons of freight. Aviation's global economic impact (direct, indirect, induced, and tourism catalytic) is estimated at $2.2 trillion or 3.5 percent of global gross domestic product (GDP). Aviation directly employs 8.6 million people and is estimated to support 56.6 million jobs worldwide.[3]

Disruption to the industry could cause significant economic and social impacts that would ripple across the globe. In addition to the lives lost, the terrorist attacks of September 11, 2001 cost the U.S. carriers over $44 billion in lost passenger revenue alone in the three years following the attack.[4] Beyond aviation, the greater economic impact of the attacks was estimated to exceed $100 billion, including effects on infrastructure, impacts to travel and business, etc. [5]

Aviation's safety culture

The aviation system is complex, highly innovative, and constantly changing. The innovative nature of the industry creates the need for a collaborative culture where members of the aviation community continually work together in a shared vision to improve safety and security. Global safety

---

[2] *Cyber Security in Civil Aviation*, Centre for the Protection of National Infrastructure, August 2012, p. 2.
[3] Aviation: benefits beyond boarders, published by Air Transportation Action Group, dated March 13, 2012
[4] Boeing study supporting TSA Risk Management Assessment Process
[3] NY Times analysis of the long-term impact of 9/1, dated Sept. 8, 2011
[5] NY Times analysis of the long-term impact of 9/1, dated Sept. 8, 2011

improvements, for example, are achieved through the efforts of organizations like the European and U.S. Commercial Aviation Safety Team (CAST) cooperating with other major safety initiatives worldwide, such as the ICAO Regional Aviation Safety Group (RASG) and Cooperative Development of Operational Safety and Continuing Airworthiness Programme (COSCAP).

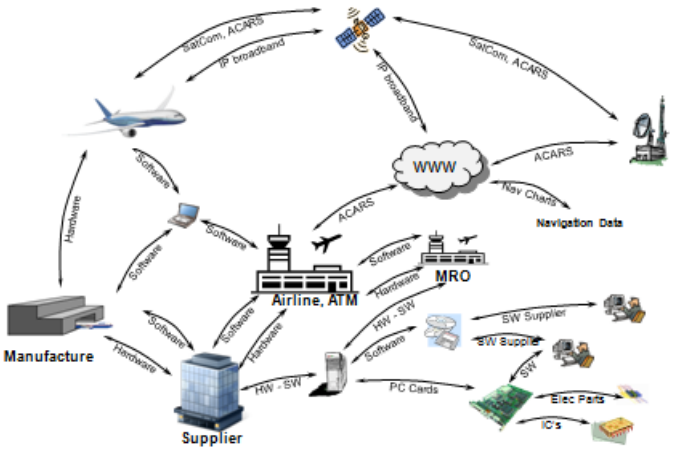
The value of this safety culture is demonstrated by the 83 percent reduction in the fatality risk achieved for commercial aviation in the United States from 1998 to 2008[6]. The model for these improvements was provided by two reports on aviation safety[7, 8] that challenged the government and industry to reduce the accident rate by 80 percent over ten years.

This risk-informed decision-making model demonstrates the effectiveness of government and industry working together to prioritize and standardize aviation safety enhancements to efficiently and effectively reduce risks. This collaborative model can also serve as a template for helping the aviation community understand the risk associated with continually implementing new innovative Information and communications technologies that may not be keeping up with safety and security measures.

Aviation and the evolution of information and communications technology (ICT)
Figure 1 summarizes aviation's **information and communications technology (**ICT) environment.

Over the years, aviation systems evolved from using proprietary tools and designs to using Commercial Off-The-Shelf (COTS) technologies. Now aviation systems use processor-based hardware and common hardware-based platforms for hosting software functionality. Specific airplane interfaces are designed into the system and easily interface with COTS technologies.

Figure 1: The ICT Environment for Aviation



Simply stated, ICT is pervasive across the aviation ecosystem, from designing and developing aircraft, to flight operations, maintenance, communications, navigation, and air traffic management.

The world has changed
This trend to increase the connectivity and interdependence of aviation systems is beneficial from a commercial standpoint, but it can present a target for those seeking to disrupt the industry and the global economy.[9]

> *The Internet's growing size, its transition from a research network operated by public entities to a commercial network operated by commercial providers who need to make a profit, and its transition from a network connecting a small community of users who trust one another to a global*

[6] Federal Aviation Administration Fact Sheet – Commercial Aviation Safety Team, dated December 11, 2011, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=13257
[7] White House Commission on Aviation Safety and Security, dated February 1997
[8] National Civil Aviation Review Commission, Avoiding Aviation Gridlock and reducing the Accident Rate, dated December 1997
[9] Ross Anderson, *Why Information Security is Hard – An Economic Perspective*, http://www.acsac.org/2001/papers/

network with users who do not know one another and may intend to harm one another put pressure on the Internet's technical foundations.[10]

I do not think today it [cyber] is necessarily the number one threat, but it will be tomorrow. Counterterrorism and stopping terrorist attacks, for the FBI, is a present number one priority. But down the road, the cyber threat, which cuts across all programs, will be the number one threat to the country. FBI Director Mueller.[11]

2) The need for a cybersecurity framework for aviation

The aviation industry is renowned for its safety record. People across the globe have come to depend on aviation as one the world's safest modes of transportation. Aviation is considered to be a highly efficient, safe, and resilient system, but people would not fly if they felt that their lives were at risk.

It is imperative that we understand the effect of security-related changes on aviation stakeholders (passengers, companies, and governments) and on the sectors of the economy that depend on air travel. To maintain a high degree of public confidence, the aviation community will need a common framework, cyber standards, and an implementation model governing the components of the aviation system. In addition, collaboration between government and industry is necessary to proactively counter aviation threats and to strengthen the aviation system's resilience against attacks.

The UK Centre for the Protection of National Infrastructure (CPNI) published a report, *Cyber Security in Civil Aviation*,[12] based on discussions of the Joint Coordination Group (JCG), which is comprised of individuals participating in standards and coordinating activities, who believe that cybersecurity should be part of all civil aviation considerations. The JCG seeks to coordinate activities associated with developing cybersecurity for civil aviation. The key findings from the report include the following:

- "The cyber world of interconnected and interdependent systems has increased the vulnerability of aircraft and systems and therefore the potential impact that breaches in security can have. More attention is therefore due to this complex but containable problem."
- "Cybersecurity vulnerabilities have the potential to jeopardise civil aviation safety and efficiency."
- "Currently, the growing threat to keeping the aviation industry safe and secure from attacks lies in cyberspace."

3) Establishing a cybersecurity framework for aviation

Ensuring a secured aviation system and staying ahead of evolving ICT threats is a shared responsibility, involving governments, airlines, airports, and manufacturers. The following framework seeks to offer an approach to increasing the effectiveness of cybersecurity for aviation. The aviation community must also develop the vision, strategy, and goals to develop the framework into a comprehensive roadmap and plan for aviation.

a. Establish common cyber standards for aviation systems
b. Establish a cybersecurity culture
c. Understand the threat
d. Understand the risk
e. Communicate the threats and assure situational awareness
f. Provide incident response
g. Strengthen the defensive system
h. Define design principles
i. Define operational principles
j. Conduct necessary research and development
k. Ensure that government and industry work together

---

[10] Barbara van Schewick, Internet Architecture and Innovation, The MIT Press, 2010, page 1

[11] Department of Defense Defense Science Board (DSB), *Task Force on Resilient Military Systems and the Advanced Cyber*, dated January 2013

[12] UK Centre for the Protection of National Infrastructure (CPNI), *Security in Civil Aviation*, Date August 2012

Framework for Aviation Cybersecurity

a) Establish common cyber standards for aviation systems

The global aviation system is now one of the most complex ICT and control systems in the world, yet there is not a recognized common vision, or common strategy, goals, standards, and practices to further safeguard aviation against the evolving cyber threats. Application of common standards or practices can help provide mitigation, including against insider threats. For example, applying common encryption standards for aviation communications could reduce the risk of interference for future enhancements to the system.

Currently there are efforts under way around the world to address cybersecurity for critical infrastructure. It is important that the aviation industry collectively shape the future legislation, regulations, standards, and practices in the areas described below. An aviation roadmap should include participation in existing forums that are developing standards for the Internet, communications, and encryption. Examples of existing standards and practices are presented in Reference 1 and Appendix A.

Information technology standards

Significant work has been accomplished in cybersecurity and additional work is under way. The NIST, the FIPS, the ISO, and the ISACA COBIT have developed standards that provide the industry with best practices. Coordinated participation in these activities by the aviation community will be important to assure that the unique requirements of aviation are considered when developing such standards.

Communications, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM)

The complexity of the global CNS/ATM system is highlighted by the existence of hundreds of service providers, which may be government owned, privately owned, or a hybrid of government and private ownership. The CNS/ATM system is also moving to a network-centric operations environment and becoming more dependent on cyber and digital technological enablers. This introduces new threats and risks, and more critical interdependencies with safety, capacity, crisis management, and critical infrastructure protection. Common policies and strategies are required. The introduction of new CNS/ATM technologies will require assuring the appropriate security layers are designed into the system. Future development must have a different approach; security must be considered for the overall cycle (concept, design, prototype, development, deployment, operation, and decommissioning). At present, some CNS/ATM systems upgrades are under study or being implemented to reduce the risk of spoofing, interference, jamming, and unlawful exploitation of signals.

Aircraft system design and production

Developing commercial airplane systems involves a structured and highly complex design and verification process, from the component level to the system and airplane level. With millions of parts on each airplane, it is critical that manufacturers ensure that the design process also address the evolving nature of cyber threats. Aircraft design must consider capabilities, threat surfaces, and cost of mitigation strategies for the lifespan of the aircraft. Secure by default must remain the industry standard.

The Radio Technical Commission for Aeronautics (RTCA), The National Institute of Standards and Technology (NIST) and the European Organisation for Civil Aviation Equipment (EUROCAE) are examples of organizations that develop standards and guidance materials used by aviation. These standards drive the certification of the safety and functionality of the design and operation, and are developed in public forums by aviation stakeholders in a collaborative, peer-reviewed environment.

Airline operations

Aircraft have a very long lifecycle, and evolve as new technologies are introduced to various systems. As a result, a new aircraft delivered today and its relevant IT systems may undergo significant reconfigurations and updates for as long as 30 years of operations. If not addressed properly, technology advances may open doors for the adversary. Secure by default must remain the industry standard.

As part of an airline's responsibility for safety, the carrier has to achieve full transparency about relevant changes to the aircraft IT components. During flight operations, the carrier has to be in the position to control all data flow into and out of the aircraft. The airline needs to agree with the

aircraft manufacturer about aircraft maintenance and operations routines that are designed to avoid cyber incidents. The aircraft developer must provide ongoing support and make the airlines aware of any potential aircraft threats or design vulnerabilities.

Ground services
The ground systems used by the airline form an important backbone for flawless airline operations. These systems include reservation, ticketing, maintenance, and baggage and cargo handling. Some of these systems may contain personally identifiable information (PII) and credit card information. Participation in the development of new standards will be important so that aviation's unique requirements are considered in the development process.

This area highlights the need for aviation to address issues that may influence the public's decision to fly, not just the ability of an adversary to prevent a flight.

Airport infrastructure
The airport infrastructure supports many functions critical for the continuity of the air transportation system. Security, power, fueling systems, and aircraft servicing are examples of services critical to airline operations. These systems continue to leverage the economic benefit of ICT. Participation in the development of new standards will be important to capture the unique requirements of airport infrastructure.

Supply chain
The interconnected global aviation system represents one of the most complex and fluid networks of systems. The nodes in this network include everything from production of aviation products to the many services required to operate airlines, airports, and air traffic services. A number of factors drive this information-intensive supply chain, including: (1) interrelated global transportation safety and security standards; (2) international alliances between carriers; (3) original equipment manufacturers (OEMs) cross-supplying and sourcing from common entities; (4) outsourcing operations and maintenance; and (5) seamless handoff of air traffic control between sectors.

Many factors are considered when designing the nodes in this system. They include: (1) strategic sourcing; (2) supply chain structure; (3) business incentive alignment and affordability; (4) supply chain architecture risk and value analysis; and (5) lifecycle value chain and control points. The role of these "nodes" in the network and the relationship between them needs to be designed, defined, restricted, and, in some cases, regulated.

To date, there are no common standards to address these considerations and ensure that the many disparate nodes that make up the complex aviation transportation sector remain interconnected. That's why the aviation industry must begin shaping the future now.

Take advantage of emerging internationally recognized standards. Consideration should be given to leveraging the work of international organizations to develop an information security and cyber protection framework that could applied to any critical infrastructure. These standards could become part of common subcontract terms and conditions for quality assurance standards.

b) Establish a cybersecurity culture
Today, commercial jetliners span the globe with unprecedented safety and reliability. The same disciplined approach that created aviation's safety culture (i.e., a common vision and strategy, clear goals, common understanding, a collaborative risk-based decision making model, non-punitive reporting structures, open communication of failures, training, etc…) must also be applied to securing cyber systems across the air transportation system. As technologies rapidly evolves, so too do our adversaries and their threats. Aviation must be prepared to adapt.

c) Understand the threat

Understand the threat actors and their intent: The aviation community must have a common understanding of these actors, their motivations, and intents to efficiently plan our defenses.

Think about the unthinkable: Our adversaries are thinking outside the box to plan cyber attacks and we must do the same to stop them. If an event does occur, (1) secure by default must remain

the standard, (2) security must be the absence of unmitigated surprises, and (3) resilient and robust systems must be in place to rapidly respond.

d) Understand the risk

Aviation has traditionally taken a risk management approach to both safety and security. The goal is to reduce risk by assessing the likelihood of the events occurring along with the consequence/ impact of the event. In cybersecurity, the risks are increasingly dynamic because of rapid technology changes, both in the systems being protected, and in the capability of the attacker. This makes it more difficult to continually assess risk in the traditional sense. Because we cannot know all of the possible permutations of attack, we must also consider system resiliency in our analysis. We must ask, "W*hen critical systems are attacked, do we understand the consequences?"*

The first step in managing cybersecurity risk is ***identifying the elements*** of the aviation system that we need to protect. The aviation system is a large and complex international entity with multitudes of stakeholders. It is highly unlikely that we can completely understand and control all aspects of the system. It will therefore be important to differentiate those areas that have only an economic impact from those areas that also have a safety impact.

The aviation community then needs to determine how to ***protect these elements*** with systems and standards. The stakeholders must protect the interfaces between major subsystems along with a system that complies with the standards and the integrity of the information, data, and products entering the aviation system. Common guidelines and standards may be possible for common interfaces.

Finally, we must understand the ***timeliness required for responding to threats*.** Changes in response to vulnerability can happen at different rates. For example, a change to a ticketing system may happen quickly as a software patch, whereas a change to aircraft software requires significantly more testing, certification, and approvals. Consideration must be given to these constraints within our response framework. Timely processes, methods, and standards for responding to an attack must differentiate the needs of each aviation subsystem.

e) Communicate the threats and assure situational awareness

Establish a protected forum for industry and government information exchange on current and emerging cyber threats to the commercial aviation system. The optimal approach to securing aviation defense is for the government and industry to collaborate, sharing threat data and sensitive information. Providing a forum where industry stakeholders can receive and share threat data would increase the speed at which threats can be mitigated across the aviation system. This gives all parties involved an opportunity to share effective countermeasures against specific attacks and adversaries. For the U.S., the Critical Infrastructure Partnership Advisory Council (CIPAC) is an existing means for government and industry stakeholders to address sensitive aviation security issues. A similar means for the international aviation community to share sensitive information must be developed.

Establish a mechanism to extend information exchange to the international community. Since the cyber threat is a global problem and international incidents can also impact the aviation system, we must establish mechanisms to exchange data with the international community. There are some unique issues here that must be addressed, such as specific countries that we should share information with and matters that may impact national security/military capability.

f) Provide incident response

Rapid incident response teams would provide the aviation community with a means to mitigate evolving threats. The security working groups such as the Computer Security Incident Response Team (CSIRT) and the Computer Emergency Response Team (CERT) are examples of organizations that have functioned for nearly two decades to response to breaches of security. The aviation community should leverage the lessons learned from other sectors to assure that capabilities to mitigate emerging cyber threats are available.

g) Strengthen the defensive system

Consideration needs to be given to strengthening ICT, including: (1) hardening the Internet backbone, including IPS malware detection and prevention; (2) securing power sources; (3) adding public-key infrastructure (PKI) or other encryption technologies; and (4) technology and procedural upgrades to critical systems. Long-term solutions may require architectural changes to aviations networks and control systems.

h) Define design principles

The design principles underlying the development of the Internet include: (1) that all nodes are known; and (2) that all nodes are trusted. These principles no longer hold true as the potential of the cyber domain continues to develop. Therefore, the advantage goes to an attacker. Aviation must define design principles for its networks and control systems that consider the evolving nature of the cyber threat. This would include identifying architectures and design principles that help us protect our systems and platforms against known attack methods, defining quality assurance standards for critical systems, and ensuring that aviation systems are resilient against unknown threat scenarios.

i) Define operational principles

These principles focus on the operational principles of systems after they are deployed in the field. This would include operational standards and best practices that mitigate threats to our systems and platforms to assure its resiliency. Items to consider would be system upgrades and patches, the timeliness of system changes, decisions on when to upgrade or retire obsolete systems, maintenance practices, access control, and personnel processes such as credentials, training, and inadvertent human errors that expose vulnerabilities that can aid an attacker.

j) **Conduct necessary research and development**

Major efforts in both research and education are under way at organizations such as CERIAS. Their experience and knowledge can be leveraged, extended, and applied to the aviation community. The aviation community, government and academia need to define and conduct necessary research and development to support the design and operational principles for enhancement to the aviation system. This would include: (1) creating secure network architectures, including methods for maintaining secure data transfer, isolating critical data, and effectively recovering from attacks; (2) determining system vulnerabilities, (3) improving attack detection, and (4) improving forensics technology.

k) Ensure that government and industry work together

Establish a governmental and industry framework to coordinate national aviation cybersecurity strategies, policies, and plans.

Establish a private/public cyber partnership that includes "business continuity elements" for the aviation sector. This would include a partnership for rapid incident response teams.

Establish policies for the near- and long-term development for cybersecurity. To encourage the aviation community to fully address the risk of cyber attacks, incentives must be tied to the solution. There must be clear benefits to implementing new security measures. The balance between market-based approaches and force of law incentives needs to be understood. An incentive-based approach may be the only way to get the market to create the behaviors that will secure critical infrastructure.

Define accepted international rules of behavior. This requires leading developed nations (e.g., the G7 or G20) to create and enforce rules of behavior for the Internet and promulgate them through appropriate treaties.

Consequences for bad behavior must be enforced. Countries that do not follow the international norms should face sanctions from the international community. Sanctions could include deep-packet inspection or prohibitions on Internet traffic from those countries.

Governments need to move cybersecurity to a high priority on the diplomatic agenda.

4) Conclusions

Commercial aviation's ceaseless pursuit of innovation has achieved an unprecedented level of reliability and safety, and a world confident in the strength, vigilance, efficiency, and resiliency of the global aviation system. However, the global aviation system is at a crossroads. Implementing ICT across the aviation system increasingly connects the global aviation system. The full implications of the increased connectivity and dependency on ICT need to be understood in light of evolving cyber threats to ensure continued confidence in aviation.

The aviation community is uniquely positioned to manage risks to its individual operations and assets, and to determine effective strategies to make them more secure and resilient. However, there is currently no common roadmap or international policy for cybersecurity in commercial aviation.

To maintain this high degree of confidence, it is imperative that the aviation community develop a common framework for governing the components of the aviation system. In addition, collaboration between government and industry is necessary to proactively thwart aviation threats and to strengthen the aviation system's resilience against attacks.

5) Recommendations

The aviation community must pursue the following course of action in light of the evolving nature of cyber threats:

- implement common cybersecurity vision, strategy, goals, and framework to address evolving threats;
- increase the cooperation and focus within the aviation community, with the active participation of all major industry players;
- leverage, extend, and apply the existing industry best practices, the response team, and the research and education efforts under,way;
- bring the appropriate government agencies into the discussion;
- begin building a roadmap by identifying near-, mid-, and long-term actions; and
- establish a governmental and industry framework to coordinate national aviation cybersecurity strategies, policies, and plans.

References

1. National Institute of Standards and Technology (NIST), Update on the Development of the Cybersecurity Framework, dated June 18, 2013, http://www.nist.gov/itl/cyberframework.cfm

Glossary

ACARS	Aircraft Communications Addressing and Reporting System A digital datalink system for transmission of short, relatively simple messages between aircraft and ground stations via radio or satellite.
ATM	Air Traffic Management
CAST	Commercial Aviation Safety Team A government and industry effort to reduce aviation fatalities through a data-driven risk management approach.
CERIAS	Center for Education and Research in Information Assurance and Security
CIPAC	Critical Infrastructure Partnership Advisory Council
CNS	Communications, Navigation, and Surveillance
COBIT	Control OBjectives for Information and related Technology
COTS	Commercial Off-The-Shelf
EURoCAE	European Organisation for Civil Aviation Equipment A European forum for resolving technical problems with electronic equipment for air transport.
ICT	Information and communications technology
ISACA	Information Systems Audit and the Control Association
ISO	International Organization for Standardization A developer of voluntary international standards for products, services, and best practices.
MRO	Maintenance, Repair, and Overhaul A provider of required air carrier inspections, heavy maintenance and overhaul of airframes, power plants, and landing gear, and modifications.
NIST	National Institute of Standards and Technology A non-regulatory federal agency within the U.S. Department of Commerce that develops technology, measurement, and standards.
PII	personally identifiable information (PII)
RTCA	RTCA, Inc. Previously known as Radio Technical Commission for Aeronautics until re-incorporation in 1991 as a not-for-profit corporation, RTCA is a U.S. volunteer organization that develops technical guidance for use by government regulatory authorities and by industry.
SATCOM	Satellite Communication A system for transmission of data between aircraft and ground stations via satellite.

Framework for Aviation Cybersecurity

Appendix A: Examples of standards used by aviation

Examples of the NIST and ISO standards used in aviation include:

- ISO/IEC 27000 — Information security management systems
- ISO/IEC 27001 — Information security management systems — Requirements
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- NIST Special Publication 800-53 — Recommended Security Controls for Federal Information Systems and Organizations

Standards that guide the development of cybersecurity measures in the CNS/ATM system include:

- DO-236 Security Assurance and Assessment Processes for Safety-related Aircraft Systems
- ICAO Annex 17- Security
- ICAO Document 9985- Air Traffic Management Security Manual

Standards that guide the development of aircraft systems include:

- NIST SP800-30 — Risk Management Guide for Information Technology Systems
- NIST SP800-53 — Information Security
- NIST SP800-82 — Guide to Industrial Control Systems (ICS) Security
- RTCA DO160 – Environmental Conditions and Test Procedures for Airborne Equipment
- RTCA DO178 – Software Considerations in Airborne Systems and Equipment Certification
- RTCA DO-254 – Design Assurance Guidance for Airborne Electronic Hardware
- RTCA DO-233 – Portable Electronic Devices Carried on Board Aircraft