Civil Aviation Cybersecurity Industry Assessment & Recommendations

August 2019

Report to the AIA Civil Aviation Council, Civil Aviation Regulatory & Safety Committee

AIA Civil Aviation Cybersecurity Subcommittee

Dan Diessner – Chair (The Boeing Company)
Hank Wynsma – Vice Chair (GE Aviation)
Leslie Riegle – AIA Leader
Patrick Morrissey – 2019 Editor (Collins Aerospace)

DOCUMENT FORMATTING

The 2019 version of this report is the second delivery of the material. An effort has been made to format the document in a manner, which would provide full context for new readers while highlighting substantive changes for previous readers who would like to focus on just the updates. Notable changes are highlighted, as done in this paragraph, to note content which has been added or modified.

Contents

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

1 EXECUTIVE SUMMARY

Today, commercial air travel is the safest form of transportation the world has ever known. Our industry has an unprecedented safety record.

Maintaining that safety performance and protecting the operations and reputation of the civil aviation industry is a shared responsibility of the global aviation community. This is accomplished by means of commonly held vision, strategies, goals, standards, implementation models, and international policies.

The same approach must be adopted for commercial aviation product cybersecurity to provide continued cyber-safety and cyber-resiliency as the aviation world becomes more connected.

As is the case with aviation safety, governments, airlines, airports, suppliers and manufacturers must work together to protect the system against aviation cyber-attacks. Accordingly, the industry needs a common aviation cybersecurity vision. It also needs to define and adopt effective international policies, and create common goals, standards and implementation models.

For years, industrial spies, terrorists, cybersecurity researchers and cyber criminals have attacked the aviation sector. As one of the most complex and integrated systems of information and communications technology in the world, the global aviation system is facing the ongoing and continuous threat of a large-scale cyber-attack. Acknowledging today's connectivity revolution, with the aviation cyber threat surface expanding exponentially due to rapid aviation connectivity growth and the ease of access to cyber tools and technologies, we must engage now with greater industry focus and vigilance to thwart cyber-criminals at all levels who would attempt to do harm.

While the existing safety regulations and standards for transport aircraft provide a robust baseline security posture, cybersecurity, cyber-safety and cyber-resiliency must be quickly and skillfully interwoven into this existing structure. Also, the wider ecosystem may be exposed to cyber-attacks, both increasing risks of operational disruption with potential significant economic impact on a wide scale. The aviation community is a globally interconnected ecosystem of both public and private stakeholders who are working to harmonize a standard approach for cybersecurity. Working collaboratively, all stakeholders need to strive to establish a common cybersecurity trust framework that includes a governance structure and technology standards that quantify the minimum expectations for cybersecurity, methods of mutual trust, and a common understanding of interoperable risk acceptance. Stakeholders must then proactively identify, understand and prioritize the risks to aviation systems in order to mitigate them.

The Aerospace Industries Association (AIA) is playing a key role by building consensus among its membership, which is comprised of the leading aerospace and defense companies. AIA currently supports three member groups addressing cybersecurity who must coordinate and leverage each other for efficiency and expediency in confronting the expanding cyber threat:

Cyber Security Committee – Exists within the National Security Policy Division and in collaboration with DoD establishes industry-wide near and long-term cybersecurity planning and policy to meet information protection requirements;

Civil Aviation Cybersecurity Subcommittee – Exists within the Civil Aviation Division and focuses on cybersecurity concerns and requirements of civil aviation including aircraft and infrastructure design and manufacturing; and

Supplier Management Cyber Security Working Group – Stands under the Supplier Management Council and serves as a mechanism to communicate Defense Department policy on how to meet information protection requirements and to share best practices among AIA's supplier network.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

Civil Aviation Cybersecurity Subcommittee presents this report and the recommendations it contains to the AIA Civil Aviation Council per the tasking at the Council meeting in April 2017. Specifically, these recommendations are actions AIA should take to address evolving threats to the commercial aviation system.

In order to assure security and prevent potential disruption to the aviation system, the aviation community should advocate that government and industry stakeholders work together to address the evolving threats and establish a cybersecurity framework for aviation. The full potential of connectivity should be securely enabled for the aviation industry. In addition, COTS, digital Field Loadable SW, and Supply Chain, are all areas that need to be considered for the risks that cybersecurity threats bring. Cyber-safety, cybersecurity and cyber-resiliency must be considered foremost when evaluating aviation connected interoperability and digital innovation.

This requires promoting U.S. -- and then international -- government and industry stakeholder support in developing the following policy priorities:

Key Policy Priorities:

- **An aviation engagement roadmap for addressing cybersecurity concerns**
- **Plans for improved secure interoperable connectivity for commercial aviation**
- **Treatment of cyber-attacks on the aviation system as unlawful interference**

2 INTRODUCTION

The recommendations in this report address evolving threats to the commercial aviation system, with a focus on the specific AIA ecosystem areas of influence encircled on Figure 1 "Securing the Aviation Ecosystem". This will include future evolving unmanned systems, both Remotely Piloted Aircraft Systems (RPAS - "in the loop") and autonomous ("on the loop"), where cybersecurity will be a key enabling technology that must be addressed up front for the design and architecture of these systems. Recognizing significant overlap in responsibilities across the ecosystem, AIA joins other stakeholder organizations such as the Airports Council International (ACI), Airlines for America (A4A), and others, so that industry has visibility over the entire shared ecosystem. This includes developing a long-term aviation vision, understanding the role of the manufacturers in the development of methodologies for the public and private sectors to work together, enabling development of a data-driven, risk-informed risk management approach for the aviation system, and defining the measures of success. The scope of this report encompasses a system-wide approach of the commercial aviation system elements within the responsibility and context of the AIA membership, in order to define the vision, the needs and the strategy. The Subcommittee has reviewed the current environment in cybersecurity, including existing standards, regulatory design requirements, and FAA requirements for the National Airspace System (NAS).

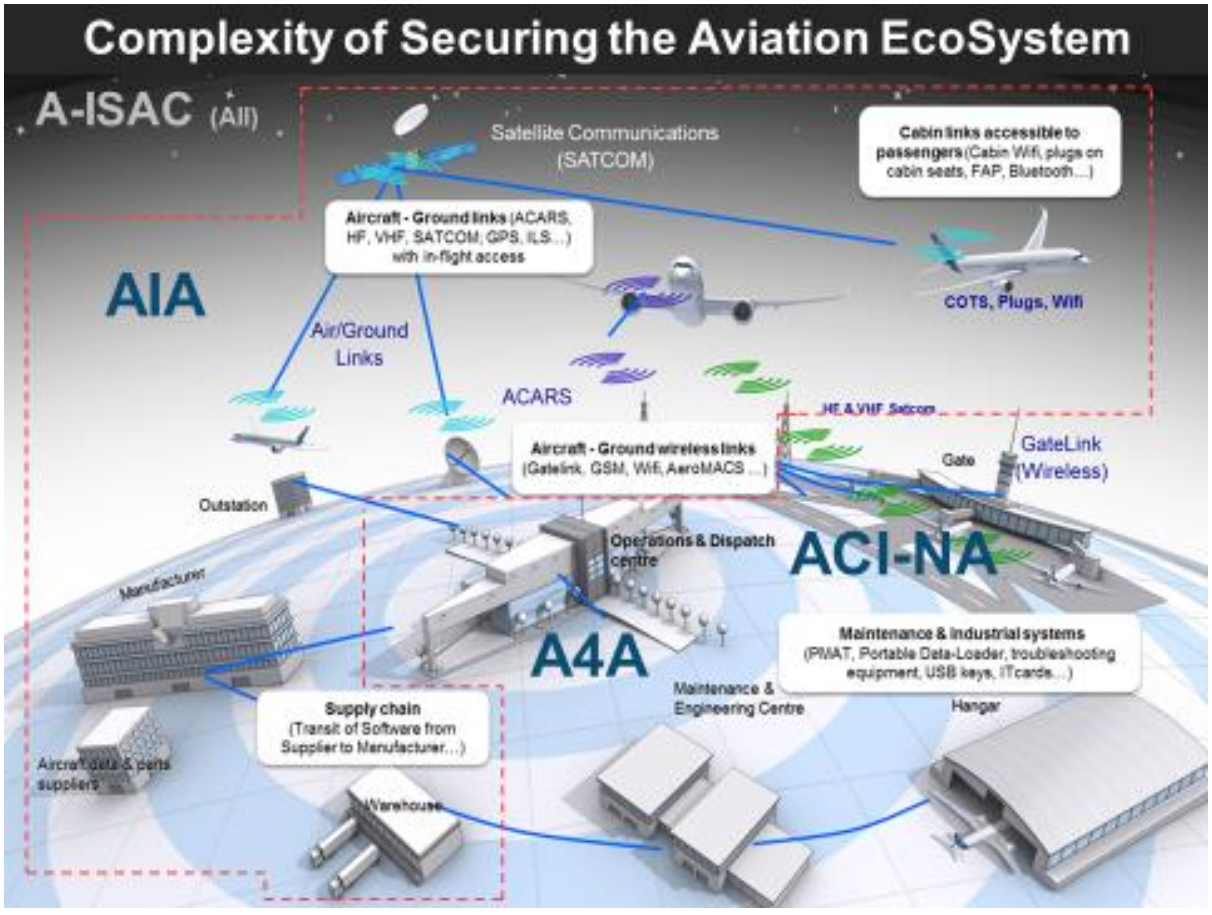

Figure 1: Securing the Aviation Ecosystem

Present State of Affairs:

- Economics drive increased automation and connectivity in aviation
- Threats continue to evolve rapidly
- Adversaries have an asymmetric advantage
- Pilots, crew, and maintenance personnel are increasingly connecting to aircraft in more complex ways
- Passengers are bringing devices with more capable computing power onto aircraft
- The internet is not secure and Internet Protocol (IP) connected systems are moving onto aviation platforms
- Increasingly complex and dynamic environment requires improved security
- Pace of technology implementation is measured in days for hackers, but in years for aviation

The implications for commercial aviation are being better understood and more deeply assessed today than ever before, creating multiple efforts to collaborate in defining standards to better secure the aviation ecosystem. Developing global standards begins with common policies for both industry and government. Without a common cybersecurity trust framework that includes both a governance structure with liabilities and a cost effective technology strategy that enables the aviation community, system disruptions and disruptions in the trust of the aviation system will likely grow, with increasing risk for a large scale economic disruption and potential safety impacts.

The aviation community can confront this threat by establishing an aviation cybersecurity trust framework for interoperability that supports the global aviation ecosystem. The aviation community must work with the appropriate government agencies to develop frameworks to address regional differences and align regional efforts for an international solution. In addition it should be a leading voice at the International Civil Aviation Organization (ICAO) in its global effort to coordinate an in international consensus via a cybersecurity trust framework aligning our specific national and regional efforts. This includes the Trusted Framework Study Group (TSFG) initiative driven by the Air Navigation Bureau and comprised of FAA, EASA and commercial industry and academic stakeholders. Also, as the European Union, the European Commission and the European Aviation Safety Agency (EASA) work to define their cybersecurity challenges and shape their effort on cybersecurity, we must pursue integration with U.S. efforts while leveraging ICAO to help secure its alignment so that we come to internationally compatible solutions. Via the ICCAIA (International Coordinating Council of Aerospace Industries Associations) we must support and bring our recommendations to the ICAO SSGC (Secretariat Study Group on Cybersecurity) and specifically the four SSGC working groups that have been formed:

- Working Group on Air Navigation Systems (SSGC/WG-ANS)
- Working Group on Airworthiness (SSGC/WG-AW)
- Working Group on Aerodromes (SSGC/WG-AD)
- Working Group on Legal (TOR to be established at a later stage)

This would generate the momentum towards achieving an international standard of behavior and consequences that are ultimately adopted by the international community. Any such effort requires a compelling, inclusive, long-term global aviation vision that clearly identifies measures of success and can rapidly adapt to dynamic threats.

The aviation community is proactively working together to strengthen the security of the aviation ecosystem, but we have significantly more to do. This report addresses an encompassing perspective of cybersecurity across the aviation ecosystem focused on the AIA scope, and has broken down this scope into the following areas to be addressed. For each section of this report, the report explores the current state, recognizing what has been accomplished, and identifies gaps to be addressed at the national and international levels through government-industry collaboration.

3 Ensuring a Product Cybersecurity Culture

3.1 Industry Commitment

To manage the threat of intentional unauthorized electronic interaction with aerospace systems and supporting infrastructure, it is imperative that aviation industry organizations fully observe the responsibility to instill a culture of product cybersecurity by establishing overall awareness, capability and readiness to protect civil aviation systems, operations and all applicable supporting infrastructure.

The recommendations herein apply to all aviation industry organizations, individuals and stakeholders involved in the development, design, manufacture, implementation, integration and support of aerospace systems and aircraft operations as depicted in Figure 1.

As mentioned previously, the European Union, the European Commission and the European Aviation Safety Agency (EASA) are working to define their cybersecurity challenges and shape their effort on cybersecurity. In particular, EASA has established the European Strategic Coordination Platform for Cybersecurity (ESCP) in Aviation. The vision is to make the entire European Aviation System more resilient and more secure to cyber threats, by adopting a through-life tiered approach to security in design, production, operations and ultimately disposal. This includes strategy, regulatory processes, and Shared Trans-Organizational Risk Management (STORM).

Recommendation: The US and other regions need to show the same industry and government commitment as the EU as they form their cybersecurity strategies.

3.2 Organizational Culture

3.2.1 Sponsorship

Enacting an effective culture of product cybersecurity relies heavily on the highest-level of sponsorship within an organization. Affirming a business level commitment to fully understand and address product cybersecurity is essential and serves as the catalyst to establishing a dedicated organizational commitment to product cybersecurity.

Recommendation: Aviation industry organizations should obtain the highest-level executive sponsorship within their business and establish a governing integrity framework to address product cybersecurity.

3.2.2 Commitment

Organizational commitment begins with a product cybersecurity governance policy that identifies stakeholder roles/responsibilities and appoints a dedicated product cybersecurity Leader to develop and maintain training, processes and tools to drive cultural change within their business.

Recommendation: Aviation industry organizations should define a product cybersecurity policy and appoint a dedicated product cybersecurity leader responsible for implementing and maintaining an effective product cybersecurity program within their organization.

3.2.3 Product Cybersecurity Awareness and Training

Product cybersecurity awareness and training are fundamental to ensuring that industry stakeholders within organizations clearly understand their role in product cybersecurity. NIST-800-53A provides widely accepted

guidance for establishing cybersecurity awareness programs within organizations for 'Information Systems' but has traditionally lacked specific focus on the unique criteria needed for product cybersecurity awareness and training programs.

To ensure the consistent application of product cybersecurity awareness and training in the aviation industry, it is important to define common expectations for product cybersecurity and hold aviation industry organizations equally accountable to establish appropriate product cybersecurity awareness and training programs.

Recommendation: Definition and adoption of industry-wide awareness guidance specific to aviation product cybersecurity, building on NIST 800-53A.

3.2.4 Capability Modeling and Benchmarking

Recognizing an aviation industry specific organizational maturity model for product cybersecurity is one means of enabling aviation organizations to independently evaluate overall capability and maturity. Advocated as a requirement, an industry recognized accreditation applied to product cybersecurity such as CMMI, NIST or ISO would provide a benchmark for organizations to achieve an effective and operational culture of product cybersecurity.

Recommendation: Aviation industry to standardize on acceptable, independently assessed capability models specific to product cybersecurity.

3.3 Product Cybersecurity Program

3.3.1 Secure System Development Lifecycle (SSDLC or SecDLC)

As part of the aviation industries' commitment to product safety, quality and reliability it is critical to recognize that equal focus is needed on product cybersecurity to more effectively cyber-resiliency of aerospace systems, aircraft operations and the interoperability between stakeholders. This is made possible by establishing a Secure System Development Lifecycle that sets forth the minimum cybersecurity requirements to ensure products, information systems and support systems are held to an equal standard of development rigor and due diligence to inherently address security related issues. See Section 4 - Establishing Cybersecurity Regulations/Standards for Aviation Systems for more information on related industry standards and recommendations.

Development methods employed should incorporate security activities into the development process to ensure security is built-in as opposed to bolted on at the end. Development processes such as Secure/Rugged DevOPS or Agile iteratively repeat design, development, validation and verification to ensure problems are found and fixed early, improving the security posture of the product and leading to cost savings.

Recommendation: Definition and adoption of industry-wide minimum development requirements specific to product cybersecurity including guidance for non-certified systems used in aerospace.

3.3.2 Product Deployment & Support

While maintaining continued airworthiness is an inherent regulatory responsibility for aviation organizations, it is imperative that aircraft OEMs, suppliers, airline operators and Communication Service Providers also develop a capability to monitor, assess and communicate product cybersecurity related incidents and concerns to assess all potential risks to aerospace systems and aircraft operations. These capabilities are key to ensuring that organizations are prepared to effectively respond in the event of a cybersecurity related incident.

Further coupling these capabilities industry-wide would serve to enhance the aviation industry cybersecurity culture, enabling an industry-wide aviation threat intelligence and information sharing working group specific to product cybersecurity. (e.g. via the A-ISAC)

Recommendation: Aviation industry organizations should establish and adopt a common incident management and incident response capability specific to product cybersecurity. (This work is being started through the efforts of SC216 & WG72 through the evolution of DO-355/ED-205, ED-201A and development of a new standard).

3.4 Documentation / Sensitive Data

Special care must be taken when communicating internally or externally concerning potential vulnerabilities. Disclosing too much information may increase the risk that the vulnerability is exploited intentionally. Accordingly, information concerning such vulnerabilities should only be shared internally and/or externally with persons having a 'need to know', and all materials concerning such vulnerabilities must be designated and secured appropriately.

Recommendation: Organizations should create processes and utilize technologies that protects sensitive product security data while stored at rest, as well as, in transit. (It is projected that Part AISS and ED-201A will address some of these topics.

4 Design and Operational Principles

Design and operational principals allow organizations and groups to function together while complying with guidance and standard documentation. Establishing these principals are essential to ensuring all products meet security standard requirements, and making sure that processes are consistent and repeatable.

4.1 Design Principles

"Design Principles" are a set of considerations that form the basis of any good product and are the backbone of organizational governance for the product design organization. Design principles help teams with decision-making. A few simple principles or constructive questions will guide a team towards making appropriate decisions.

An appropriate set of design principals should consist of:

- Roles and Responsibilities – This should clearly establish the scope and responsibility for each group within your organization and design team.
- Product Cybersecurity Development Life Cycle Data – Clearly defined documents and data to be generated during your development program, this could include cybersecurity threat assessments, security verification methodologies, testing plans, results, etc. The group responsible for both the generation of the life cycle data, stakeholders, and approvers should be clearly identified.
- Best Practices/Standard Operating Procedures – This should include workflow definitions, definitions for inter-functional group interactions, step-by-step instructions for common activities.
- A Safety Risk Assessment (SRA) Product Cybersecurity Process – An aviation systems organization needs a repeatable SRA methodology that consistently and correctly identifies and prioritizes security risks associated with aircraft systems. The SRA methodology must include guidelines, procedural steps (that exercise careful analysis), testing, and strategy in order to assess the systems safety risk and advance up-to- date airworthiness security and protection. The SRA process is part of the regulatory compliance for aviation product development and support.

- A Business Risk Assessment (BRA) Product Cybersecurity Process: To ensure the efficiency and viability of the aviation industry and each organization's business operations, an aviation systems organization needs to assess overall product cybersecurity risks to the business. The SRA is a subset of the BRA, and while the BRA's non-SRA elements are mostly an unregulated activity they are still critical for enabling ongoing smooth operations. The NIST Cybersecurity Framework assessment process provides a reasonably mature and robust method that can be applied or adapted to product cybersecurity at the organization and aviation industry levels.
- Test Methodology Definition – Testing should encompass both requirements based testing to verify security requirements have been implemented and met per design, as well as, include robustness testing that provides evidence of cyber resiliency to vulnerabilities and attempted cyber penetration.
- Work Flow Standards – Standard work-flows need to be defined
- Traceability to Standards – All company design principals should show trace coverage to industry standards to ensure that both the letter and intent of these standards have been meet
- Plan for Continued Airworthiness – In addition to meeting the current standards for Instructions for Continued Airworthiness (ICA), considerations should be made to address continuing cybersecurity threats as they evolve over time and as design changes evolved the security perimeter.

4.2 Operational Principles

Operational principles act as a navigation aid, which provide continual guidance on how an organization needs to operate in order to meet their express security objectives. They can help provide an objective foundation to ensure the organization is operating in accordance with industry standards and internal procedures and a basis for determining any mid-course corrections that may be required. Part AISS, as well as DO-355A/ED-204A, are expected to address many of these principals and it is particularly relevant for participants in the operational data supply chain for the aircraft such as ANSPs.

An appropriate set of operational principals should consist of:

- Infrastructure Requirements
    - IT Security Policy – Ensure that corporate policies are compliant with NIST/Industry Standards and that there is a policy for monitoring and updating as required, and support/interface properly with the product security requirements and policies to meet business needs.
    - Physical data security – Ensure that corporate policy and action supports physical data security, including physical access to electronics, lab equipment, factory equipment, and data; in accordance with both IT security and product security requirements.
- Continuing Education
    - Compliance Training – Ensure that all employees are trained on corporate security policy and formal records keeping for both IT security and product security.
    - Continued Learning – Training programs to educate designers on new security threats
        - Public/Private Partnerships – Partnering with government and/or universities to exercise case studies, etc.
- Industry Group Participation – Develop strategies and plans for industry group participation
- Internal Audit Program – Implement independent and internal auditing to ensure compliance with internal and industry standards.

4.3 Summary

Historically, our industry has very successfully used design and operational principles to satisfy safety criteria and business expectations. The aviation ecosystem, including the air navigation system and aircraft, are being networked and equipped with advanced connectivity technology for broader integration and interoperability. The importance of cybersecurity for all elements of the aviation ecosystem has emerged as a new industry challenge. Networked systems provide the ability to access and share real-time data for responsive decision-making and control. These networked systems also enhance safety, increase efficiency, and provide cost savings for airlines, but they open potential susceptibility pathways to attacks that could impact the air navigation system and aircraft operations. Understanding the broad disruptive potential of these cybersecurity attacks, it is critical to incorporate correct cybersecurity measures and make and enforce policies for systems implementation to ensure a safe and efficient aviation ecosystem. To this end, aviation systems manufacturers need to establish appropriate design and operational principles in order to consistently and effectively prioritize and manage the cybersecurity risks of the aviation ecosystem.

5 Establishing Cybersecurity Regulations/Standards for Aviation Systems

This section addresses considerations and recommendations for industry regulations, standards and guidance that are within the scope of AIA. At a high level, and aligned with the ICAO Industry High-Level Group recommendations, National Institute of Standards and Technology (NIST) and International Standardization Organization (ISO), standards are encouraged as they often lead to lower design, development, and certification costs.

The FAA and EASA are developing regulations and supporting the creation of standards to formulate, extend, leverage, and apply best practices to the design and operation of cyber-resilient digital aviation systems. These extensive efforts have been primarily focused on protecting critical system and preventing propagation via low assurance systems with “network” connectivity that might provide a beachhead into more critical systems. However, less emphasis has been put on addressing gaps in Communication, Navigation, Surveillance (CNS) and Air Traffic Management (ATM) elements such as ACARS, GPS, ADS-B, ground infrastructure and secure end-to-end communications (including those for safety services), ILS, etc. All of these require a trusted interoperable operating environment that will integrated airplane and airspace operational approach.

In addition to the specific items below, the AIA Civil Aviation Cybersecurity Working Group fully supports the recommendations of the August 2016 final report from the Avionics Rulemaking Advisory Committee (ARAC) Aircraft Systems Information Security / Protection (ASISP) working group to the Federal Aviation Administration.

While there are many areas that we need to work together to address, the following are the current top priorities:

5.1 Aeronautical Information System Security Design, Development, and Operation

RTCA SC-216 and EUROCAE WG-72 have jointly produced industry standards on airworthiness security process specification, information security guidance, and airworthiness security methods.

- ED-201A “Aeronautical Information System Security (AISS) Framework Guidance” (Draft, scheduled to be released 2020)
- DO-326A/ED-202A “Airworthiness Security Process Specification” (Final)

- DO-355A/ED-204A "Information Security Guidance for Continuing Airworthiness" (Draft, scheduled to be released 2020)
- DO-356A/ED-203A "Airworthiness Security Methods and Considerations" (Final)
- Future DO-xxx/ED-xxx "Information Security Event Management" (Draft, scheduled to be released 2021)

In addition, EUROCAE WG-72 has produced these industry standards.

- ED-205 "Process Standard for Security Certification and Declaration of ATM ANS Ground Systems" (Final)

Other standards related to design development and operation:

- **ATA Spec 42:** *Aviation Industry Standards for Digital Information Security*
- **ARINC 811:** *Commercial Aircraft Information Security Concepts of Operation and Process Framework*
- **ARINC 664:** *Aircraft Data Network, Part 5 – Network Domain Characteristics and Interconnection*

Recommendation: RTCA and EUROCAE should look at ways to simplify the standards with a clear focus on cyber-safety with built in flexibility. Harmonization should continue to be a priority.

The FAA is addressing when Special Conditions (SCs) are required for aircraft systems and networks for three main areas:

- Connecting portable Electronic Flight Bag (EFB) systems to aircraft control display units
- Field loading of software parts to aircraft systems
- In Flight Entertainment (IFE) System connectivity to aircraft systems and networks

In addition, to ensure the end-to-end cybersecurity across the ecosystem from the ground to the airplane, all elements must be examined as a part of the security analysis from initial point of access to the target system. Thus it is important that all systems in the path be available to incorporate defense in depth to implement layers of security and be considered as part of the accredited security analysis.

For example, often lower design assurance aircraft systems, i.e. DAL D and DAL E systems, or even ground systems, are not considered because by definition they have minor or no safety effect. However, lower design assurance airplane systems and ground systems often have the largest threat surface and ability to provide the first critical security layers for providing defense in depth. If those lower design assurance systems connect to higher design assurance systems, i.e. DAL C and higher systems, and/or those lower design assurance systems propagate the threat, then they should be an accredited part of the end-to-end security assessment, and encouraged to implement security measures that are part of the security assessment.

One of the strategies to increase the security on lower DAL systems, as called out in DO-356A, is the concept of Security Assurance Level (SAL), which is a classification for the confidence in the protection and resilience of the aircraft and aircraft systems provide against attacks. The SAL determines the rigor applied to the product and the development process to avoid vulnerabilities and to demonstrate the effectiveness of security measures and the security architecture as evaluated in the security risk assessments. It is assigned to security measures and assets. The SAL process is very similar to the traditional safety processes. It varies in that it includes security objectives and considerations that aren't covered by traditional safety processes. By separating SAL from DAL it becomes possible to incorporate strong security mechanisms in lower cost system enabling attacks to be stopped nearer to the edge of the aircraft as opposed to them be permeated through.

Recommendation: Even though higher design assurance systems are expected to have the appropriate security measures and be able to protect themselves, it is recommended to stop the threat sooner and implement security measures at the point of access, regardless of the design assurance level of that point of access, to include security measures in the connecting ground systems.

5.2 Electronic Flight Bag (EFB)

The FAA has published an issue paper on Portable EFB connectivity to aircraft systems as well as the EFB Advisory Circular (AC 120-76D, issued October 27, 2017) on security considerations. EFB security guidance is challenging because it is not Part 25, but some aircraft systems enable bidirectional communication with safety related systems. This AC is currently under revision to provide stricter guidance, an update is expected out later this year.

Recommendation: Next update of EFB AC needs broader and more in-depth industry review and input. Encourage the operators (via the regulators and/or industry collaboration) to control the EFBs.

5.3 Field Loadable Software (FLS)

ARINC Software Distribution and Load (SDL) working group published the ARINC 827 and ARINC 835 standards (Guidance for Security of Loadable Software Parts using Digital Signatures) regarding use of digital signatures to detect and prevent software tampering. The Aviation Rulemaking Advisory Committee (ARAC) published a final report with recommendations on FLS in August of 2016. The ARAC FLS recommendation has been used to update DO-355 and FAA AC 43-216 regarding operator software management practices. AC 43-216 applies to all aircraft, while AC 119-1 (which references DO-355) applies to connected (eEnabled) aircraft.

Recommendation: AIA should encourage industry and regulatory collaboration to define specific policies and guidelines to be applied to all aircraft software.

5.4 In-Flight Entertainment (IFE)

FAA has policy and guidance on the installation of IFE systems in transport category airplanes. Additional work is being done by the ARINC Cabin Systems Subcommittee (CSS). This subcommittee's work includes developing interface standards to allow airlines to implement preferred systems for their passengers. Cabin communications, connectivity, wireless distribution, cabin interface protocols, and connector standardization are all intricate components of this activity. The growing complexities and scope of cabin equipment has resulted in the expansion of ARINC 628.

Recommendation: Ensure security is considered by this subcommittee and appropriately incorporated into the next revision of ARINC 628. Also ensure there is a cybersecurity focal actively participating in the writing of new upcoming ARINC standards, e.g. Onboard Secure Wi-Fi Network Profile and Media Independent Aircraft Network Communications.

5.5 Non-trusted Services

In PS-AIR-21.16-02 Rev. 2, the FAA will issue Special Conditions for aircraft systems connecting to non-trusted services and networks, including airport gate link networks (e.g. Gatelink), cellular networks, and portable electronic devices (e.g., EFBs)

Recommendation: Guidance has been identified for EFBs, but it is also needed for the other non-trusted services.

5.6 Logging

ARINC 852 "Guidance for Security Event Logging in an IP Environment" leverages industry best practices to provide guidance for aircraft manufacturers, equipment suppliers, and operators. The scope of this guidance applies to networks and systems residing in the Airline Information Services (AIS) and Passenger Information

and Entertainment Services (PIES) Domains. However, it does not address non-security related logging that could be leveraged for security forensics, non-IP networks, Aircraft Control Domain (ACD) systems, or specific implementation details.

Recommendation: Evaluate potential value of security logging requirements at the airplane systems level. Consider evaluation across all connected systems, potentially incorporating additional elements from both AIS and ACD domains, and including the use of existing systems event logs in the context of cybersecurity.

Additionally, WG-72 & SC-216 are working on information security event management (ISEM) guidance in a collaborative effort. Complimentary to ARINC 852 which, addresses log creation and processing, the new guidance document will provide recommendations for aggregation, processing and evaluation of those logs to identify potential security events and respond to them.

Recommendation: Consider greater guidance regarding the responsibility of the operator for ongoing log analysis.

Recommendation: Long term plan for WG-72 is to work on a forensics/restoration standard. A means should be explored for how to bring some of this work forward without impacting ISEM timeline.

5.7 Air Traffic Management (ATM)

The ICAO Trust Framework Study Group (TFSG) (formerly INNOVA) is underway to provide a common aviation trust framework establishing a common set of principles, policy, and guidance, and a transition strategy for a globally harmonized framework that will enable trusted ground-ground, air-ground and air-air exchange of data and information among relevant aviation stakeholders with the level of resilience and interoperability needed to support increased capacity and efficiency for the continued safe operation of the civil aviation system, and consider and incorporate future industry needs for both existing airspace users and new entrants (i.e. UAS / RPAS) in the aviation system while ensuring the globally harmonized trust framework takes into account relevant technologies, including the Internet infrastructure, for the exchange of information in support of air traffic management and flight operations.

The TFSG is focused on developing realistic and achievable methods to securing the interoperability of the global aviation community. This will require support from all aviation stakeholders. However, TFSG has identified that having an entity to build the initial framework becomes a key success factor in being able to move forward. Recognizing that ICAO is not an operational organization or technical body, TFSG will focus on establishing a governance and compliance structure with a trust framework that can be leveraged by the aviation community as a whole.

The TFSG project objectives will be to define and establish a structure, developed through partnership with industry, that enables the aviation community to apply a common set of principles promoting minimal operating standards for ground and communications systems for cyber-safe operations and cyber-risk accepted methods for interoperability for trusted and reliable information exchange.

The TFST is developing a concept of operations that describes the basic principles of its trust framework and identifies how they are applied to the aviation community through standardization of specific technical controls for identity management and risk reduction and a supporting governance structure.

The TFSG team is proposing to:

- Work directly with industry forums and ICAO WGs to leverage work for governance and technical standards already being performed to accelerate the process of establishing more explicit ICAO guidance on cybersecurity that is mutually agreed to across the aviation community.

- Leverage the efforts of the Secretariat Study Group on Cybersecurity (SSGC) for establishing the guidance that defines the minimum operational standards (NIST, ISO 27000, or others) for cybersecurity that each aviation stakeholder would establish for the operations and management within individual operating boundaries.
- Working with the technical stakeholders to leverage the work being completed by the community today (PKI, IP addressing, DNS, et al.) to standardize and implement the technical solutions described.

For the global aviation community of users, these simple principals can only be accomplished when supported by the technical community (RTCA, EUROCAE, SESAR, FAA NextGEN, AIA, Aircraft and avionics Manufacturers, Airline Operators, etc.) and the regulating bodies to help drive new policies. The scope and scale of the TFSG will provide a foundation for managing risk across the aviation community as a whole, enable the community to establish common networks for interoperability, define methods to effectively manage risk and establish a foundation that will be required to fully realize the capabilities of SWIM and services such as FF-ICE, 4D Trajectory, etc. If the communication can work together, the outcomes from the TFSG project will allow organizations to simplify integration that is currently very complex, and to reduce cost of operations.

EUROCAE WG-72 Subgroup ED-205 has developed an approach (published in 2019) to assessing end-to-end risk of ATM systems that will be used for *Security Certification of ATM Systems within Europe*. However, this is work that does not have a counterpart in the US yet.

Recommendation: AIA should be involved with EUROCAE efforts, and work to define an appropriate US forum for better addressing cybersecurity for CNS/ATM systems. Now that RTCA is no longer an advisory committee to the FAA, one possibility is for them to work jointly with EUROCAE on a future revision of ED-205. Another possibility is US guidance on ATM security coming from SAE.

Recommendation: Ensure ED-205A or ED-205 supplement explains assurance levels as they relate to the implementation of security measures; and addresses event monitoring, incident handling, and information sharing to collaborate around incident management in the aviation network as incidents arise.

AIA has a seat on the European Commission's Industry Consultation Body (ICB). The ICB is a platform for the definition of the future ATM strategy and its implementation, and provides all major stakeholders in the European ATM industry with an opportunity to express their views to the European Commission (EC) and the Member States. It does this by providing position papers and giving technical advice to the EC on the implementation of Single European Sky (SES) initiatives and legislation.

Recommendation: Ensure that ATM future data communications and equipment mandates appropriately address cyber-safety, cybersecurity and cyber-resiliency and have a solid business case.

5.8 Internet Protocol Suite (IPS)

The Existing ACARS and ATN/OSI infrastructure for aeronautical safety services is unique to aviation and will not scale based on the forecasted increase in passenger air travel. Additionally, these aeronautical networks were developed at a time when cybersecurity was not a design consideration and as a result, do not include security provisions. To achieve greater efficiencies in air traffic management, as well as to resolve the existing security deficiencies a new aviation communication network, based on the Internet Protocol Suite (IPS) is being developed. However, the use of IP based communication also increases the risk of an airplane safety event being induced via cyber means. To solve these challenges, standards bodies across all levels of aviation need to work together to securely design and implement IPS. The ICAO WG I Communication Panel, the Mobility and IPS Security Subgroups, RTCA SC-223 IPS & EUROCAE WG 108, and AEEC IPS Subcommittee are

carrying out this work. Together they are coordinating to define the performance, technical and certification requirements for IPS.

ARINC has developed an industry roadmap development plan for defining IPS for Aeronautical Safety Services, including airborne, ground-based and space-based communication systems, coordinating with aviation Standards Development Organizations (SDOs), Air Navigation Service Providers (ANSPs) and others with an interest. Current work is focused on developing the box level requirements and architecture to support IPS.

FAA IPS Security Subgroup along with ICAO WG-I are developing secure communications standards for the next generation of aeronautical safety services. This work will advance data communication technologies used for NextGen and SESAR airspace initiatives and, in turn, provide a number of benefits to airlines, airframe manufacturers, and avionics suppliers. Robust digital link security will provide enhanced capabilities which are not a part of today's system capabilities, such as secure primary ATC communications over digital communications links. Airline benefits are expected to accrue in the form of greater data communication performance compared to ACARS and ATN.

RTCA SC-223 and EUROCAE WG-108 are coordinating closely with both the AEEC/ARINC and ICAO IPS efforts. ICAO Document 9896, Edition 3 provide both high level requirements and operational context. ARINC Specification 858 for avionics, currently in draft, intends to define the Internet Protocol Suite (IPS) for Aeronautical Safety Services. In addition to the profiles document, the group is creating a Minimum Aviation System Performance Standard (MASPS) for IPS for avionics certification.

ARINC Network Infrastructure and Security (NIS) develops standards for IP connectivity and security to the aircraft and enables fleet-wide solutions based on open standards for lower development cost, increased flexibility, higher reliability, reduced complexity, longer lifespan, and ease of configurability and maintenance. NIS is to harmonize network-related and security-related activities of the various AEEC subcommittees working in related areas. This should reduce redundant activities, implement better more consistent, flexible, and interoperable solutions, provide for better configuration control and ease maintenance.

Recommendation: Monitor WG-I activities (including DOCs 10094 & 100095) to help shape ICAO policy level efforts and drive standards developed by ARINC, RTCA, EUROCAE and FAA working groups in the right direction for maximum benefit with appropriate cybersecurity solutions.

5.9 Aircraft-Ground Links, SATCOM

ARINC Air-Ground Communications System (AGCS) Subcommittee ensures that current and emerging satellite air-ground communication systems are aligned with airline operational requirements and defined for cost-effective implementation based on existing and anticipated aircraft architectures. Updated AGCS SATCOM standards will lead to improved network performance, increased uniformity in data link service provider interfaces, and expanded air traffic services. Other standards include ARINC 781 and 771. Additionally, the air transport industry benefits from this standardization via the continued competition among communications service providers.

Inmarsat/ESA Iris Project is a multi-year Inmarsat project funded by the European Space Agency that will define the technical and operational requirements for aeronautical safety services over Swift Broadband SATCOM for Europe.

Recommendation: EASA is planning to mandate the Inmarsat/ESA Iris Project requirements for aeronautical safety services over Swift Broadband SATCOM for Europe, and Airbus is planning to implement this on their airplanes. Recommend understanding and shaping these requirements as they will ultimately apply to all aircraft operating in Europe. Regarding aircraft-ground links, stay involved in standards developed by ARINC.

5.10 Continued Airworthiness (CA)

Many companies address continued airworthiness (CA) challenges and ongoing CVE (Common Vulnerabilities & Exposures) evaluations through standard software block points, service bulletins, etc. However, there is limited guidance in this area at the box or LRU (line replaceable unit) manufacture level, which might, for example, be associated with maintaining PMA. With the drafting of NPA-2019-01 this year the first rules for continued airworthiness are staged to take effect. While the rules themselves provide little detail they set the regulatory baseline that CA needs to be addressed in the context of connected aircraft and provided from the OEM to the operator. Part AISS provides guidance in setting up an organizational structure to support cybersecurity in systems including to address CA. AC-43-216 Software Management During Aircraft Maintenance and AC-119 Operational Authorization of Aircraft Network Security Program (ANSP) provide guidance on the protection of the digital maintenance process and the development and management of a ANSP. Additionally, AC-119-1 describes an acceptable means of obtaining operational authorization for an aircraft certified with a special condition (SC) related to security of the onboard computer network. AC-119 also references ARINC 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework which contains guidance on airplane security aspects for continued airworthiness.

Recommendation: Develop cyber-safety regulations, standards and/or guidance to which all companies are held for maintaining continued airworthiness. This should include monitoring and evaluation of their products for applicable vulnerabilities of their products during the life of the product.

Recommendation: A lack of guidance in what should be included in the ICA provided by OEMs and suppliers has led to challenges for the operators in developing the necessary programs to provide adequate supporting processes. A committee (such as A4A) could take up the effort to develop some standard guidance on what should be included in the ICA and the format to convey the information in to be most effective.

Recommendation: Utilize draft DO-355A/ED-204A to include this guidance and help the operators write their ANSPs. Provide ANSP guidance on how airlines should handle the log data that the aircraft provides as well as OEM response to log findings. Generate a new standard for OEMs (and perhaps others) to have an ISMS to ensure security is considered in all relevant aspects of design and operation.

Recommendation: Capture necessary incident response processes and activities in DO-xxx/ED-xxx.

Recommendation: Develop strategy for rapid identification and resolution for CVEs that affect onboard airplane systems and avionics (patching).

5.11 Return to Service of Aircraft

With the threat of cyber attacks on aircraft, standards on how to detect and report an attack as well as some aspects of responding to an attacks are in development. WG-72 has included forensics on their standards roadmap to identify how an attack has occurred and the extent of its impact. Airlines have expressed an interest on penetration testing aircraft. For both cases, a method on how to return such aircraft into revenue service needs to be established so that a known good state can be re-established and airworthiness restored. Industry, in combination with intelligence provided by government agencies, should decide upon the level of effort needed to reinstall aviation equipment. Whether it is sufficient to simply reload the operational software, if it is necessary to return the equipment to shop and do a full low level reinstall using JTAG and similar component level programming, or if the only recourse is to scrap the equipment.

Recommendation: Aviation industry to standardize an acceptable return to service policy using inputs from government and intelligence agencies. Engage with standards bodies and regulators to advocate for guidance in this space either through standards or regulations to provide a foundation for this work.

5.12 Software

Airplane software is considered an airplane part including the code controlling complex electronic hardware often referred to as firmware. But the regulations and standards do not adequately account for the flexibility and ease of update (malleability) of software consistently across legacy and modern aircraft. AC-43-216, Software Management During Aircraft Maintenance, was written to drive consideration of this problem; DO-355, Information Security Guidance for Continued Airworthiness gives summary direction to operators for the managing the security of ground support systems and the software distribution process. But more effort is needed to provide more tangible guidance to the industry participants for managing the complete lifecycle of the data & software supply chain for the ecosystem.

AIA has provided a detailed analysis of software security, in particular the secure delivery from origin to the aircraft. Resulting from the analysis, recommendations have been made for the near, mid and long term to improve security of software throughout the aviation ecosystem and lifecycle.

Recommendation: In summary, Industry recommends that end-to-end secured software delivery is implemented for all aircraft (including legacy) and that ARINC establish a standard for secure data loaders (work underway). All data loaders, including those of Field Service Engineers, should be secured appropriately. Industry also recommends establishing a commonality for digital signatures built off the Trust Framework in discussion with ICAO. A more detailed version of these recommendations are being developed concurrent to the publishing of this report.

5.13 Supply Chain Audit

There is currently no consistent guidance on securing the supply chain suitable for both civil and defense purposes. With the general threat to aviation with its complex supply chains and also specific items of legislation being drafted globally that will require considerations of supply chain security, industry needs to establish means for securing the aviation supply chain.

AIA has provided a detailed analysis of supply chain and split the problem into manageable sections. For each section, recommendations are provided on securing the supply chain.

Recommendation: In summary, Industry recommends that an objective-based standard be developed for securing Operational Technology that uses existing standards as a basis. Industry also recommends harmonizing existing standards for identifying fraudulent components into one approach for civil and defense purposes. SAE G-32 Cyber Physical Systems Security committee should be consulted as the primary standards development organization working on supply chain security. A more detailed version of these recommendations are being developed concurrent to the publishing of this report.

5.14 NIST Standards

NIST maintains mature standards for the development and management of computing technology. Many of these standards are being utilized in federal regulations and programs today to guide development and operation of cyber-exposed systems. The below NIST standards are commonly referenced in program and product requirements for federal systems:

- 800-30 – Risk Management Guide for information technology systems
- 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems
- 800-53 – Recommended security controls for federal information systems

- 800-53A – Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- 800-115 - Technical Guide to Information Security Testing and Assessment
- 800-160 - Systems Security Engineering -Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- 800-181 - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

Recommendation: Review NIST standards available today to identify those which should be referenced in a regulatory or advisory capacity to enhance aviation cybersecurity.

Recommendation: Review NIST standards addressing new and evolving technology and the potential cybersecurity impacts. For example, Draft NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.

5.15 ISO Standards

As the aviation industry is a late adopter of digital technology and communication, many standards have been developed for the risk assessment, development, and operation of digital connected systems. Standards organizations such as ISO maintain mature standards for the development and management of computing technology. Two such standards are:

- ISO-27001: Information Technology – Security Techniques – Information Security Management Systems Requirements
- ISO-27034: Information Technology – Security Techniques – Application Security – Overview and Concepts

Recommendation: Review ISO standards available today to identify those which should be referenced in a regulatory or advisory capacity to enhance aviation cybersecurity.

5.16 European Cybersecurity Standards Coordination Group (ECSCG)

Europe has established a coordination group to ensure we do not duplicate or neglect standards/standardization areas in the area of cybersecurity. This should be supported to ensure quality standards but also tie in with recommendations to FAA that such strategies should be duplicated in the US. In fact, Action 01-07 states, "ECSCG activities shared with AIA. AIA is attempting to have US replicate EU activities (e.g. equivalent to ESCP and ECSCG)."

Recommendation: AIA work with ASD on mapping of cybersecurity and cyber-related industry guidance and activities. ASD is an active member of European Cybersecurity Standards Coordination Group (ECSCG), so AIA should coordinate with ASD to communicate this mapping and present a unified industry voice.

Recommendation*: AIA recommends Aircraft Cybersecurity Initiative (ACI) to take the leadership to form an equivalent organization to what is being done with ECSCG to coordinate the various standards efforts across the US and then coordinate with ECSCG to help ensure collaboration and reduce duplication*.

5.17 Cyber Safety Commercial Aviation Team (Cyber Safety CAT)

The aviation safety culture within the United States has attained an unprecedented measure of success resulting in a flying public that has little concern regarding of aviation safety. The emphasis and prioritization of safety has developed an aviation culture with a solid understanding of safety issues and well-structured safety management systems that effectively mitigates safety risks. The aviation community has also been driving e-enabled efficiencies and services throughout the aviation ecosystem that capitalize on expansive growth of computing and connectivity technologies. The companion growing concern is that the e-enabled aviation ecosystem could be targeted by malicious actors attempting to negatively influence the reliability, integrity and availability in ways that could impact safety. The need to blend the success of the aviation safety culture with the developing aviation cybersecurity culture has resulted in the aviation community to focus attention on the cyber safety concerns. A need for a well-structured formal aviation security consortium similar to the existing Commercial Aviation Safety Team (CAST) has surfaced.

This Cyber Safety Commercial Aviation Team (Cyber Safety CAT) concept document is intended to capture the need and to initiate a government and industry consortium, which will address aviation cyber safety risks across the aviation community. The consortium will establish a network of trusted aviation entities with formalized communication channels that will raise the cyber awareness within the aviation community by working together in a structured proactive approach. The Cyber Safety CAT will utilize a common data driven Risk-Based Decision Making (RBDM) management approach with resources reaching across the aviation community. The well-structured approach will increase efficiencies in the aviation community and enable the aviation community to explore cyber safety use cases that cross the aviation ecosystem to include aircraft, airline flight and maintenance operations, airport aircraft ground operations, air traffic management systems and other key aviation stakeholders.

Figure 2 Cyber Security Awareness is Rising

The Cyber Safety Commercial Aviation Team (Cyber Safety CAT) will provide a well structure aviation cyber safety forum to complement the existing Commercial Aviation Safety Team with the following:

Vision: Key aviation stakeholders acting cooperatively to lead the US aviation community to the highest levels of commercial aviation cyber safety by focusing on scenarios that enable proactive and continuous assessment of vulnerabilities and risks to the aviation ecosystem.

Mission: Enable a continuous improvement framework built on the proactive identification of current and future cyber safety risks, develop mitigation recommendations and monitor the effectiveness of implemented actions.

Goal: Reduce the U.S. commercial aviation cyber safety risk, improve cyber resilience, and continue to work with our international partners to reduce cyber safety risk world-wide.

Deliverables: Actionable mitigation recommendations for best practices, awareness, technology development, standards, EASA/ESCP harmonization, ICAO influence, support to aviation cyber safety incident communications & response plans, guidance, policy, and if needed recommendations for regulatory consideration.

The data driven approach will also result in the ability to have an aviation industry wide consensus on aviation risks and mitigation strategies on various cyber safety concerns. The benefit to the aviation stakeholders will be to ensure a continued resilient civil aviation system where we will work proactively to establish solution based approaches to counter cyber safety risks and maintain the confidence of the flying public. The consortium will propose mitigations of cyber safety risks to the flying public whether they be associated directly with an aircraft, its operations and maintenance, or the efficiency of the air traffic management system. In addition to providing a greater margin of safety, other benefits are anticipated in the reduction of overall risks such as: reduced loss/delay of operations to avoid a frustrated public, reduced risk of harm to the aviation industry reputation, and reduced negative impacts to the US and global economy, as well as better recommendations for appropriate government oversight.

On March 6th 2019, the key US aviation cybersecurity leaders from industry and the US government met at the AIA Headquarters in Washington DC and agreed to move forward with this US Cyber Safety CAT definition effort. This included the US OEM industry (via the AIA Civil Aviation Cybersecurity Subcommittee) and the US government (including the ACI DHS/FAA/DOD Tri-Chairs, FAA cyber leaders from aircraft/operations/airspace, and other ACI DHS leaders).

Recommendation: AIA to work together with industry and the FAA, while coordinating closely with the Aircraft Cybersecurity Initiative, in establishing and maturing Cyber-Safety CAT, as well as collaborate with the EU and ESCP as the initiative matures.

5.18 Other Aerospace Standards

Some standards such as ARP4754A, DO-178C, DO-160 and DO-254 do not contain cybersecurity specific requirements. However, industry can (and has) leverage this guidance for cybersecurity, and should consider if any changes are needed to these documents so that Cyber-Safety is adequately addressed.

ICAO Secretariat Study Group on Cybersecurity (SSGC) created working groups in the following areas that will lead to policy guidance, standards and regulations for civil aviation: Current and Future Air Navigation Systems, Airworthiness, Aerodrome, and Legal. These working groups will influence international standards.

Recommendation: Via the ICCAIA (International Coordinating Council of Aerospace Industries Associations), AIA should support and bring our recommendations to the ICAO SSGC (Secretariat Study Group on Cybersecurity) and specifically the four SSGC working groups being formed. AIA currently has representation on SSGC Working Group on Current and Future Air Navigation Systems and SSGC Working Group on Airworthiness.

The first plenary of the Trust Framework Study Group (TFSG/1) was held at ICAO Headquarters in Montréal, Canada from 6 to 10 May 2019. Mr. Eric Vautier, Airports Council International (ACI)) was nominated as chairman of the TFSG, and TORs were approved. The Study Group will:

a) develop a common set of principles, policy, and guidance, and a transition strategy for a globally harmonized framework that will enable trusted ground-ground, air-ground and air-air exchange of data and information among relevant aviation stakeholders with the level of resilience and interoperability needed to support increased capacity and efficiency for the continued safe operation of the civil aviation system; and

b) consider and incorporate future industry needs for both existing airspace users and new entrants in the aviation system while ensuring the globally harmonized trust framework takes into account relevant technologies, including the Internet infrastructure, for the exchange of information in support of air traffic management and flight operations.

ICAO Trust Framework Study Group has created three working groups: Digital Identity Working Group (DIWG), Trust Reciprocity Operational Needs (TRON) and Global Resilient Aviation Interoperable Network (GRAIN).

Recommendation: Via the ICCAIA (International Coordinating Council of Aerospace Industries Associations), AIA should support and bring our recommendations to the ICAO Trust Framework Study Group (TFSG) to guide and strengthen the TFSG overall, and support the three working groups.

The current SSGC is under the Air Transport Bureau and the TFSG is under the Air Navigation Bureau. AIA recognized that ICAO needs an entity to address and integrate cybersecurity horizontally across ICAO organization. Therefore, AIA fully supported the development of the ICCAIA Working Paper to the 40th ICAO Assembly recommending ICAO to "Create a civil aviation cybersecurity entity, governed by member states with the support from industry that can work transversally across ICAO organizations to consolidate and harmonize cybersecurity related activities across ICAO". See below ICCAIA Proposal Regarding ICAO Governance Structure for Cybersecurity summary:

EXECUTIVE SUMMARY

Civil aviation cybersecurity is a broad, complex and multi-disciplinary field which encompasses aspects of information technology, traditional aviation security, safety management and impacts to aviation operations. Because cybersecurity is transversal, ICAO's current panels and study groups are not effective at coordinating activities like cybersecurity. There is a need to establish an ICAO entity, governed by member states with the support from industry, which is not constrained by the existing ICAO organizational structure. This entity should have the ability to ensure that all cybersecurity activities are effectively coordinated across ICAO and that interfaces of cybersecurity with other disciplines are appropriately managed. This entity should be responsible for a common ICAO strategy for cybersecurity and to align and orientate work being performed by existing panels and study groups.

Action: The Assembly is invited to:

1. Create a civil aviation cybersecurity entity, governed by member states with the support from industry, that can work transversally across ICAO organizations to consolidate and harmonize cybersecurity related activities across ICAO,
2. Adopt the cybersecurity strategy developed by the SSGC, while recognizing that the SSGC was not structured to address the horizontal and crosscutting nature of cybersecurity,
3. Coordinate with States and industry to harmonize the cybersecurity risk management processes, taking into account the harmonization work already done at regional or national levels,
4. Encourage states of various regions to develop cybersecurity crisis management capacities and to coordinate at the international level to prevent the loss of passengers trust due to a local aviation cybersecurity incident.

Overall recommendation: Establish appropriate policies and standards to support a balanced cybersecurity implementation across the global aviation ecosystem.

Overall recommendation: In addition to the cybersecurity industry guidance and activities discussed in this section, AIA to track new industry guidance in evolving technologies like IoT, RPAS, and Wireless Avionics Intra-Communication (WAIC) systems to ensure there is no cybersecurity gap.

6 Understanding the Threat

On November 4 of 2015 there was an outage in the Swedish air traffic control system which resulted in the cancellation and redirection of flights destined for or originating from the Arlanda, Landvetter and Bromma airports. During this time air traffic controllers' screens went dark leaving them unable to provide situational awareness or direction to pilots operating in their airspace. At the same time, Sweden notified CERT authorities within NATO of an ongoing significant cyber-attack. Though the source and nature of the event have not been officially confirmed many believe the timing of the notification and the occurrence of the outage were not coincidences.

Regardless of what you believe was the source of the outage, cyber-attacks on the aviation infrastructure are happening today. They may occur at a smaller scale and in most cases mitigated before there a systemic impact. As noted by both the US and EU governments, the airspace system has been identified as critical infrastructure to be considered on par with water, and energy control systems. The recent WannaCry ransomware attack reinforced this point that critical infrastructure such as transportation is vulnerable.

As the aviation infrastructure becomes more and more connected, systems like NextGen are modernizing Air Traffic Management with greater connectivity to provide benefits like more direct flights, lower fuel consumption, etc. However, with increased connectivity and information exchange comes increased cyber risk. Many aircraft flying today and the air navigation systems that support their operation were developed long before cyber threats were a significant consideration. As such, some parts of the aerospace system may be more vulnerable than others.

At the outset, the task of characterizing the threat seems daunting. In a software driven world where lines of code measure in the millions, it is difficult to imagine how to account for all the possible bugs and design flaws which might represent a vulnerability. Multiply those numbers by the thousands, millions, or billions of computing systems that make up the international airspace system and its participants and the task of securing the environment may seem unmanageable.

To be successful it is important to break the problem down into the most common elements. Although types of attacks and their impact can be widely varied taking forms such as denial of service (DOS), advanced persistent threats (APT), malware, or zero-days (to name a few), they all originate through a similar vector. All cyber-attacks utilize information flows.

RTCA DO-356A defines the term, Intentional Unauthorized Electronic Interaction (IUEI) to describe threats to the aircraft system: "a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems, but does not include physical attacks such as electromagnetic jamming."

Fundamentally, cyber systems consume, process, and transmit information; because of this, it is also how they are vulnerable. From this vantage point system designers and operators must evaluate the system in terms of the system interfaces and the data those interfaces consume. Furthermore, they must evaluate the source and content of the data and how it might be altered to negatively affect the system. It is in this context the threats to the system can be fully understood. In security circles, this is referred to as a threat model and it is composed of a set of common features: Assets, Actors, Trust Boundaries, Information Flows, and threats.

This approach to modeling the system is critical in the analysis of the system's threats and helps the system designer and maintainers have a common language through which they can discuss how to identify, evaluate, and mitigate the threats revealed.

Recommendation: The digital development community has created formal approaches that aviation stakeholders can use for modeling threats to (and within systems) through Attack Trees and DFD Threat Models. AIA needs to advocate for the use of these methods in the documentation of systems to help facilitate common language in how we discuss and resolve threats to the aviation ecosystem.

For managers of operational systems, additional approaches are required to understand and discuss attacks in progress and the evolution of threat, to compromise, to embedment of a malicious cyber-actor. The most common method for discussing an attack in progress is found in the Cyber Kill Chain developed by Lockheed Martin. The Cyber Kill Chain defines the 7 steps of a cyber-intrusion as follows:

- Reconnaissance: harvesting information about the target, this could be through network scans or research of publically available information about employees, the company, or the asset.
- Weaponization: coupling an exploit with a backdoor into a deliverable payload.
- Delivery: delivering the weaponized bundle to the victim via email, the web, USB, etc.
- Exploitation: exploiting a vulnerability to execute code on a victim's system.
- Installation: installing malware on the asset
- Command & Control: establishment of the command channel for remote control of the malware on the embedded system.
- Actions on Objectives: execution of primary attack objectives, such as: exfiltration of data (IP theft), denial of service, ransom, etc.

Recommendation: Industry stakeholders need to have common language and methodologies for communicating the state of a cyber-attack to manage its advancement and minimize propagation. This can be done via EASA ESCP and the upcoming Cyber-Safety CACASRT. Companies and the aviation community need to be knowledgeable how to utilize the Cyber Kill Chain in prevention and response to protect the aviation ecosystem.

The rest of this section is provided to provide the reader with a summary discussion of the components of a threat model

6.1 Assets

Assets are the elements of a system that have value, they may be whole systems, functions within a system, or at the lowest level pieces of data. In DO-356A (aviation context) it's defined as the logical and physical resources on of the aircraft including functions, systems, items, data, interfaces, processes, and information. They are the target of a threat because of the value they provide. For instance, an autopilot system is an asset because if the function was lost there would be an impact to the operation of the aircraft. Assets are typically characterized in terms of security properties, namely: availability, integrity, and confidentiality to define what is important about the asset. Some discussions of security properties break these three into finer grained detail but the three are commonly accepted. The security property is important because it indicates what about the asset is critical in operation and will dictate how a threat to the asset must be mitigated. In the case of the previously mentioned autopilot a security property of availability would be assigned to the asset and additional autopilot systems would be added to the design to ensure the function is always available.

The security properties typically are defined as follows:

- Availability - the characteristic of a function or data which dictates it is accessible when it is needed.
- Integrity - the characteristic of a function or data which dictates that it is only changed or altered through a controlled trusted process.
- Confidentiality - the characteristic of a function or data which dictates it can only be accessed by authorized functions or actors.

6.2 Actors

Actors are the people or systems which interact with the system being modeled. Actors in a threat model are evaluated as trusted or untrusted based on who they represent. A pilot is a trusted actor in an aircraft system but the EFB they carry may not be depending on how it's controlled and if it could be infected or compromised.

PS-AIR 21.16-02 (used to clarify the need for special conditions related to cyber security) defines untrusted actors with an aircraft system as "non-governmental services", providing examples of Gatelink, public networks (e.g., internet), cellular networks, PEDs, EFBs.

This definition is problematic in that it is too US centric. In many parts of the world, parts of the airspace system management and its services are privatized, resulting in a lack of clarity.

Recommendation: Work with standards bodies to define and incorporate a more universally applicable use of trusted & untrusted actors within the aviation ecosystem, and possibly define a detailed specific list of trusted and untrusted actors.

6.3 Trust Boundaries

Trust boundaries define the physical or logical boundaries of a system across which data is exchanged. Trust boundaries can be defined at any level and clarify which interactions with a system are trusted (and do not require assessment or evaluation) and those that are untrusted, representing possible threats to the system. Untrusted boundaries exist between the system and untrusted actors while trusted boundaries exist between trusted actors and the system.

6.4 Information Flows

Information flows define what information is sent or received by the system. All information flows must be understood to develop a complete picture of the system being modeled to expose all possible threats to the system. Directionality in information flows is important as it is used to further understand what types of threats could exist in the information flow. For instance, if an asset has a property of confidentiality, caution should be taken to ensure only the permitted information is leaving the system. To the contrary if an asset has a property of integrity, risk comes from data flowing into the system. Information flows also help identify access and pivot points for an attacker.

6.5 Threats

Once the model is complete and the above elements are accounted for, threats in the system can be more clearly understood. Anywhere data flows from an untrusted source into an asset or a system which provides access to an asset a threat could exist. From an aircraft perspective, threats can take many forms:

- Over-the-air-attacks (Spoofing vulnerable components – e.g., navigation receivers)
- Malware (introduced by diagnostic equipment)
- Compromised components (infected microcontrollers or remote terminals introduced by supply-chain attacks)
- Lateral compromises (via another infected aviation system exploiting implicit trust)
- Unwitting crew members from their personal devices

But if a threat model can be defined for the system they can be formally documented and better understood. With that understanding comes clarity on how to address them.

In April of 2015 a report from the GAO recommended holistic threat models be developed to help strengthen cybersecurity in the Airspace system. "Twelve of our fifteen cybersecurity experts discussed enterprise-level holistic threat modeling, and all twelve agreed that FAA should develop such a model to strengthen cybersecurity agency-wide. NIST and the twelve experts we consulted said that threat modeling, a cybersecurity best practice, enables an organization to identify known threats, including insider threats, across its organization and align its cybersecurity efforts and limited resources accordingly to protect its mission."

As mentioned in the GAO report the existence of a threat model enables the operators, administrators, and designers of the systems to fully understand the threats to a system at each level and likewise prioritize mitigation of those threats in the face of limited resources.

Recommendation: Develop/recommend a holistic threat model for the airspace system to help standardize the definition of what information within the system is trusted and what information flows represent a possible threat vector. Doing so will help suppliers and OEMs be more cohesive in the development and management of the systems that make up the NAS.

7 Understanding and Managing the Shared Risk

To manage cyber risk, it is imperative that the industry and government partners work together to identify the elements of the aviation ecosystem that most need protection. The aviation ecosystem 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. EASA ESCP Shared Trans-Organizational Risk Management (STORM) work stream is one example of how industry and government partners are working toward this.

By properly characterizing the aforementioned systems (and functions), we can also evaluate the criticality of those functions in the overall system context and likewise better characterize the risk they present in the context of a cyber-attack. In designing and managing systems it will be important to understand what level of risk is acceptable in any risk assessment that's performed to ensure some components of the system aren't more vulnerable than others leaving a gap in the overall system defensive readiness.

Recommendation: Engage aviation industry stakeholders to define and prioritize cybersecurity risks to be addresses for the aviation ecosystem. Leverage our safety culture and history by establishing a joint government and industry commercial aviation security team, similar to what we did with the Commercial Aviation Safety Team (CAST) which developed an integrated, data-driven strategy to reduce the commercial aviation fatality risk in the United States and promote new government and industry safety initiatives throughout the world. This Cyber-Safety CAT is currently under development.

There are many standards provided today for risk evaluation but ultimately the designers, owners, and operators are responsible for making choices about what levels of risk are acceptable and what threats must be mitigated. Because assumptions and assessments will need to be validated for all systems, it will be necessary for the certification authorities and industry participants to speak the same language and agree upon what level of risk is acceptable within each of the operational domains.

What standards for risk assessment should be used? While there are indeed many available methods, one method of assessment may be preferable to another in specific areas. For instance, assessment and risk evaluation of ground support IT systems might prefer a method more tailored to IT environments whereas a separate method may be appropriate when evaluating embedded airborne systems.

By establishing cyber security risk management framework standards for commercial aviation systems, the industry will develop an increased awareness of the threats and risks. With this knowledge, organizations can implement policies, procedures, and controls to better secure their systems. This will create a demand for the knowledge and skillsets needed to do the work which will drive the cyber-security culture forward.

Recommendation: Monitor the development of risk management focused working groups to support and encourage leveraging existing standards such as NIST.

8 Communicating the Threats and Assuring Situational Awareness

In the aviation ecosystem, as with cybersecurity in most domains, managing threats and events effectively requires a response plan which expands beyond company boundaries. While the aviation industry is fiercely competitive on the retail level, keeping rates low and the quality of service high, competition can inhibit event mitigation or resolution. Ineffective communication or information isolation puts everyone at risk. Imagine a police department investigating a home invasion gang in its city and not sharing the information with the surrounding communities.

The aviation industry is prone to shared risk more than any other industry. Companies can only manage the cyber risk within their reach, yet they are subject to the cyber risks of key partners. As such, an airline can manage all its risk well and yet suffer millions in losses if its planes are stuck at an airport which did not manage its cyber risk well and vice-versa.

The security culture in the aviation Industry, particularly in the cyber arena, must be more open and cooperative within the bounds of an aviation trust framework. The sharing of intelligence will only happen where there is an established foundation of trust between all key aviation stakeholders. Companies must build trusted relationships in order to comfortably share information about successful attacks against their infrastructure and agree to not use that information competitively. A highly successful model is the Aviation Information Sharing and Analysis Center (A-ISAC). In just 5 years, they have built a trusted community of aviation companies headquartered on five continents. The community is growing at a steady rate as it continues to score wins for companies through its intelligence sharing program.

The US government has several initiatives to collaborate with the private sector. Under PPD-21, DHS and the private sector collaborate on cyber and physical threats as grouped under Critical Infrastructure (Aviation is a sub-sector within the transportation). The Aviation Government Coordinating Council and its private sector equivalent, the Aviation Sector Coordinating Council collaborate on setting strategies and initiatives to reduce risk to the sub-sector. Some of these initiatives include the Air Domain Awareness and Analysis Cell (ADIAC). Other initiatives such as the Aviation Intelligence Strategy Board, the Interagency Core Cyber Team (ICCT), and ADS-B Working Group have also increased government and private sector collaboration on critical cyber issues. As a result, the public-private engagement has improved dramatically over the past year.

In 2017, there was an effort within the government to consolidate initiatives and resources into a more efficient model for prioritization and achieving outcomes. As the private sector owns and operates the majority of the aviation eco-system in the US. The private sector has vast cyber intelligence capabilities and skills which can leverage and even enhance government cyber threat intelligence.

Recommendation: The government must continue to work toward exchanging more unclassified, relevant threat information with the private sector. This includes methods for sharing actionable unclassified information about known vulnerabilities identified in classified programs.

ISACs are remarkably effective in the intelligence world. However, ISACs did not exist when the security clearance policies were developed decades ago. Many ISACs have staff which would benefit from classified briefings, however due to rules which do not fit the current models for intelligence sharing, ISACs are barred from getting clearances as they do not qualify as security facilities. ISACs do not need to maintain or store classified information, however key analysts within these communities would be able to better protect the sector and provide enhanced intelligence to the USG if they were cleared. This problem must be rectified.

Recommendation: The government needs to review and update the policies regarding clearances within the ISAC community to foster better information sharing and situational awareness.

9 Incident Response & Mitigation

Beginning in 2015 with the Black Energy attacks on the Ukraine and now continuing into 2018 with exposure of new WPA2 Krack and Meltdown-Spectre vulnerabilities, the Civil Aviation Industry must improve its ability to respond to incidents from new threats that seek to exploit vulnerabilities to critical software and hardware for aviation industry operations. With the advent of the "Internet of Things" and machine learning, Incident Management for Civil Aviation must rapidly expand beyond enterprise level protections into protecting aviation industry products and operations, operational technology, and supply chain product cybersecurity.

The purpose of Product Cybersecurity Incident Management is to rapidly identify and characterize cybersecurity concerns to enable aerospace industry partners and stakeholders to effectively manage and minimize potential safety, operational, and financial impacts from both credible and perceived risks and/or incidents affecting the Aviation Ecosystem. For safety and airworthiness of aircraft, the definition and reporting requirements for an incident are defined in 49 CFR Part 830 Parts A and D respectively (see airworthiness recommendation in Section 4.10 "Established Cybersecurity Regulations/Standards for Aviation Systems - Continued Airworthiness".

Recommendation: In addition to the specific recommendation to evaluate 49 CFR Part 830 for potential updates for Cyber-Safety (see Section 4.10), more generally consider horizontal and crosscutting guidance spanning the entire aviation ecosystem to address incident reporting and information sharing for cyber-safety, cybersecurity and cyber resiliency. It will be important to have a balanced approach of guidance, regulation, and support for the aviation industry sharing, and not overregulate for non-safety related incidents by allowing the industry to manage anonymized sharing of information via the Aviation ISAC. Guidance can be partially addressed via the upcoming DO-xxx Information Security Event Management document.

The goal of incident management is to develop the effective methods and coordination tools needed to significantly improve partner and stakeholder incident management capabilities in order to reduce cybersecurity risks to the Civil Aviation Industry.

In order to accomplish this task, AIA should leverage existing service communications and tools employed by the Aviation Information Sharing and Analysis Center (A-ISAC) to improve aviation industry cybersecurity incident response and coordination with partners.

To make these efforts successful, AIA and its aerospace industry partners must maintain a continuous cycle of interdependent activities for Cybersecurity Incident Management, including;

- Developing Aviation Industry goals, objectives, and strategies for managing and responding to cybersecurity incidents across the industry
- Maintaining Cyber Safety (compliance with Safety & Airworthiness Certification)
- Preparing and coordinating Aviation Industry activities and reviews to support risk and impact analysis as detailed in section 6 "Understanding and Managing the Shared Risk".
- Addressing standards for coordinating communications among Aviation Industry partners and government stakeholders, as detailed in section 7 "Communicating the Threats and Assuring Situational Awareness".
- Evaluation of potential safety, operational, and financial risks and specific impacts to Aviation Industry and its stakeholders
- Developing and implementing effective Action Plans to obtain both near-term and strategic resolution

- Documenting actions to address cybersecurity concerns, including archiving incident related data, decisions, and lessons learned for future use.

Recommendation: AIA and our aviation industry stakeholders must move rapidly to define, develop, and validate effective Incident Management policies and processes to proactively manage product cybersecurity incidents. Leverage the strengths and expertise of our industry to maintain the cyber safety, cybersecurity, and cyber resiliency of the aerospace industry and strengthen our defenses.

10 Strengthening the defensive system

Strengthening the cyber security posture of a system means reducing and hardening the attack surface and underlying system in order to preserve the operational integrity, availability, and/or confidentiality of the system's assets.

The commercial aviation ecosystem is a system of complex systems (see Figure 1: Securing the Aviation). There are many systems and components needed to ensure its proper function: aircraft control, airline information management, passenger information and entertainment services; information supply chain components such as airline operation centers, database and weather vendors; maintenance & industrial system suppliers, and the devices passengers bring onto the aircraft, to name a few. With the evolution of technology, these systems have become both more digital and connected over time. As with other information management and digital systems, modern aviation critical infrastructure requires a layered, holistic approach to provide a defense-in-depth architecture in which all components of the commercial aviation system contribute to the security of the NAS. Evidence of this need is echoed in many places.

In April 2015 the GAO produced a report titled 'FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen'. Findings from this report recommended the implementation of a "well developed holistic cybersecurity threat model and continuous monitoring program" to help ensure the cyber-resiliency of NAS.

Recommendation: Leverage existing standards and policies to encourage a system-wide holistic approach by industry participants to strengthen digital systems in the aviation ecosystem for improved the system's cyber-resilience. (see section 4 "Establishing cybersecurity regulations/standards for aviation systems" for specific standards recommendations.)

Many industries, and specifically the defense industry, are being required to meet cyber-security standards for the control and management of both IT and product systems that should continue to be leveraged. The department of defense (DoD), which has close ties to the aviation ecosystem, has developed policy guidance for the DoD acquisition process which addresses the full life cycle protection of weapons platforms. This guidance states that the DoD "must strengthen lifecycle protection policies, enterprise implementation support, and R&D programs to ensure that DoD weapon systems are designed, fielded, and sustained in a way that reduces the likelihood and consequences of cyber supply chain attacks".

Recommendation: Leverage DoD investments and developments where possible. A good place for the AIA Civil Aviation Cybersecurity Subcommittee to start will be to coordinate formally with the two AIA DoD focused cybersecurity forums (AIA Cyber Security Committee & Supplier Management Cyber Security Working Group).

One good first step to strengthening the defense system is to conduct a thorough end-to-end cybersecurity assessment (architecture and vulnerability) with the FAA, its partners, OEMs, airlines and the aftermarket. (NOTE: See recommendation in Section 5 "Understanding and Managing the Shared Risk" for establishment of a Cybersecurity effort similar to CAST to develop an end-to-end cybersecurity assessment.) These types of system-wide holistic assessments often take the form of table-top exercises which help serve the stakeholders by exposing not only threats and vulnerabilities, but dependencies and process gaps which can be critical in

mitigating active threats. A good table-top exercise would include representation from the regulatory agencies, air traffic control personnel, the supply chain, passenger systems, aircraft and air traffic control systems, baggage claim systems, and even maintenance. Similar events have been coordinated by the A-ISAC, and soliciting cooperation with the A-ISAC in these efforts would be highly advantageous and productive.

Recommendation: AIA should encourage participation in the A-ISAC in all forums to help grow the membership and likewise expand communication and sharing of intelligence.

Manufacturers today are investing in the development of the next generation of design and operational principles to strengthen the security posture of commercial airplanes which includes the systems that support the airplane operational environment. Because the defensive strength of a system is a function of the sum of its parts it should be evident that individual components within the NAS system must be developed, built, and administered with the appropriate rigor to ensure their operational integrity. To facilitate this, security must be considered earlier in the design process starting with architectural assessments early in the design phase. The architectural assessment would encompass developing the threat models as described above in Section 4 "Understanding the Threat".

Once the threat model is complete a vulnerability assessment can be conducted focused on all significant vulnerabilities related to the most critical elements emulating various attack capabilities to understand the system's security posture.

Finally, via the Cyber-Safety CAT like forum, work as an aviation community to mitigate discovered vulnerabilities using a top down priority risk management framework approach:

- Prioritize identified security gaps or vulnerabilities based on risk
- Propose and model mitigations
- Implement technical and non-technical improvements (i.e., software patches, security products or services, modified operational and maintenance policies and procedures, training)
- Test and monitor results
- Iterate as needed

In summary, the iterative process associated with the Mitigation step allows for the use of a large set of countermeasures, depending how cyber resilient the strength of the defensive system is modeled to be. Countermeasures can be technical or procedural depending on the threat and the system.

11 Key Policy Priorities

The aviation industry must establish policies that define minimum cybersecurity standards for all aviation ecosystem stakeholders (public and private) to maintain and implement across their unique operating domains, and then validate on a regular basis. This will include policies that define minimum standards of risk acceptance for interoperability and connectivity between aviation stakeholders. To this end, the three immediate key policy priorities listed below encompass and support the materials and recommendations from the body of this report.

- An aviation engagement roadmap for addressing cybersecurity concerns
- Plans for improved secure interoperable connectivity for commercial aviation
- Treatment of cyber-attacks on the aviation system as unlawful interference

A summary of primary messages of this report for addressing cyber safety, cybersecurity and cyber resiliency of the aviation ecosystem are:

- ✓ Need to generate an "Aviation Culture of Cybersecurity Awareness" across all stakeholders.
- ✓ Need to establish appropriate policies and standards to support a balanced cybersecurity implementation across the global aviation ecosystem.
- ✓ Information sharing is critical to our success. (Aviation ISAC identified as example to leverage.)
- ✓ Government to Industry sharing hampered by classification constraints. Need appropriate method for sharing actionable data.
- ✓ Need a risk managed approach to address existing gaps and to architect future secure systems.
- ✓ Need better global visibility and collaboration to address aviation ecosystem threats and risks.
- ✓ Contribute to the Cyber-Safety CAT initiative to develop and end-to-end view of cyber security and risk in the ecosystem.
- ✓ Next generation systems must be architected/designed with cybersecurity in mind.

11.1 Developing an Engagement Roadmap for Addressing Cybersecurity Concerns

The governments and industry must work together to develop a framework and roadmap for coordinated regional and then global aviation cybersecurity strategies, policies, and plans. The first step in building the roadmap must start with a discussion among the key stakeholders focused on developing a common understanding of the needs and priorities. As discussed in detail throughout this recommendations report, areas of consideration for the roadmap should include:

1. developing common definition of threat sources and assets within the aviation ecosystem
2. enhancing intelligence sharing of threats and assuring situational awareness
3. strengthening incident response/management capabilities
4. building a research and development plan for securing the next generation of connectivity
5. defining international norms of behavior to establish a legal framework

Assuring the future safety and security of the global aviation system in the face of increasing cyber threats requires an approach that recognizes both the political and technical considerations. Addressing the political considerations requires a plan to align the US government stakeholders first and then extend the effort to like-minded nations.

The charge for AIA and the Civil Aviation Cybersecurity Working Group is to first establish an engagement roadmap starting with industry and government US stakeholders, and then expanding to Europe and leveraging ICAO via the ICCAIA. For example, ICCAIA should work collectively with ICAO to establish a more definitive aviation engagement roadmap within the Global Air Navigation Plan (GANP) for addressing cybersecurity concerns. While the AIA Civil Aviation Cybersecurity Working Group will need to build out the details of the engagement timeline, a prospective plan for key stakeholder engagement is outlined below:

11.1.1 Prospective US Industry Engagement Plan & Stakeholders

Engage the appropriate US industry stakeholders to bringing them into the discussion in developing a "one industry approach":

Steps:

a. Share AIA recommendations report as a starting point for discussion
b. Develop Working Together proposal
c. Engage US industry stakeholders
d. Solicit feedback on the key issues to address in developing the roadmap

e. Participate to the creation of the Cyber Safety Commercial Aviation Team initiative
f. Update the Working Together proposal as appropriate

US Industry Stakeholders – Some Areas of Common Interest (and include others when identified):

- A-ISAC (Aviation Information Analysis and Sharing Center) – Information sharing is the A-ISAC focus applicable to: understanding the threat, understanding the risk, communicating the threats and assure situational awareness, providing incident management, developing a roadmap for addressing cyber security concerns. A-ISAC has a similar roadmap initiative that extends across the entire ecosystem, and should be the key industry partner for collaboration on an aviation cybersecurity roadmap and coordination of aviation ecosystem elements beyond the scope of AIA.
- A4A (Airline 4 America) - Connectivity devices used by crew and maintenance personnel, and the interfaces to the airplane.
- RAA (Regional Airline Association) - Connectivity devices used by crew and maintenance personnel, and the interfaces to the airplane.
- ACI-NA (Airport Council Int., North America) - Communications links to the airplane such as Gate Link (wired & wireless), AeroMax, etc.
- Miscellaneous Standards Organizations – see report section on recommendations for standards.

11.1.2 Proposed US Government Engagement Plan and Stakeholders

Engage the appropriate government agencies bringing them into the discussion in developing a joint government and industry approach:

Steps:

a. Share AIA recommendations report as a starting point for discussion
b. Develop Working Together proposal
c. Brief key government stakeholders on the proposal to develop an integrated Roadmap for Aviation and advocate for a Government/Industry Working Together approach to develop an integrated Roadmap for Commercial Aviation
d. Solicit feedback on the key issues and the appropriate mechanism for developing the roadmap
e. Define approach to bring a joint government and industry approach to developing the roadmap
f. Update the Working Together proposal as appropriate

US Government Stakeholders (include others as identified):

- DHS (Department of Homeland Security) Leadership
  - DHS CSIA (Cybersecurity and Infrastructure Security Agency)
  - DHS S&T (Science & Technology)
  - TSA (Transportation Security Administration)
  - AGCC / ASCC (Aviation Government Coordinating Council / Aviation Sector Coordinating Council)
- ODNI (Office of Director of National Intelligence)
  - NAI2O (National Aviation Intelligence Integration Office)
- DOT (Department of Transportation)
  - FAA (Federal Aviation Administration)
    - FAA CISO
    - FAA Cyber Regulatory
    - FAA Tech Center
- NTSB (National Transportation Safety Board)

- DoD (Department of Defense) – USAF (United State Air Force)
- NSA (National Security Agency)
- Congressional Engagement: Transportation & Infrastructure, and Commerce Committees.

11.1.3 International Collaboration

- ICCAIA Security Committee
  - Work through the ICCAIA to facilitate reach to ICAO, ASD, EASA, etc.
  - Provide input into Part-AISS, ESCP, and NPA-2019-01 to build the vision for commonality in guidance and regulation in line with a one-industry approach.
- ICAO (International Civil Aviation Organization)
  - TFSG (Trust Framework Study Group)
  - SSGC (Secretariat Study Group on Cybersecurity)
  - ANB (Air Navigation Bureau)
  - ANC (Air Navigation Commission) Panels
    - e.g. Airworthiness Panel, Air Traffic Management Operations Panel, ATM Requirements & Performance Panel, Communications Panel, Information Management Panel, Navigation Systems Panel, Remotely Piloted Aircraft Systems Panel, Surveillance Panel, etc.
  - ATB (Air Transport Bureau)
  - AVSEC (Aviation Security) Panel

11.2 Develop improved secure interoperable connectivity for commercial aviation:

The U.S. and Europe should create a research and development (R&D) plan focused upon the next generation of secure connectivity for the commercial aviation system. The full potential of connectivity should be securely enabled for the aviation industry. In cases of doubt, security and safety must overrule connectivity and digital innovation. A critical enabler for success will be agreed upon cybersecurity standards across aviation systems, where key recommendations have been identified throughout but primarily in section 4 "Establishing cybersecurity regulations/standards for aviation systems". At the policy level this will include working with ICAO to support SSGC efforts and working groups.

11.3 Treat cyber-attacks within the context of unlawful interference:

The FBI uses 18 U.S. Code section 1030 – Fraud and related activity in connection with computers. The Aviation Transport Security Act 2004 - SECT 10 defines unlawful interference with aviation, but it is unclear how this is incorporated into regulations. More must be done in this area to discourage would be attackers. Governments must advocate for the International Civil Aviation Organization (ICAO) to develop the necessary instruments to treat cyber-attacks on the aviation system as unlawful interference. As in the case of an act of terrorism on an aircraft -- which is currently recognized as an unlawful interference -- cyber events on aircraft and the Air Navigation System are also acts that jeopardize the safe and orderly operation of civil aviation and therefore must receive equivalent recognition in the legal framework of ICAO nations. Through Assembly Resolution A39-19, ICAO recognizes that not all cybersecurity issues affecting the safety of civil aviation are unlawful, but there must be a clear statement defining intentional unlawful interference vis-à-vis cyber security. Key instruments to achieve this goal are the *Convention on Offences and Certain Other Acts Committed on Board Aircraft* (Tokyo Convention) and Annex 17, but today's situation might call for a more encompassing framework that includes the Air Navigation System and ground infrastructure in addition to the airframe. This same resolution highlights the importance of partnership with industry in cybersecurity, so this

presents an important opportunity. ICAO SSGC has identified a working group to address legal aspects of aviation cybersecurity, and during the SSGC-2 meeting it briefed as "TOR to be established at a later stage".

Recommendation: Work via ICCAIA to express the priority for ICAO to develop new and/or modify existing necessary instruments to treat cyber-attacks on the aviation system as unlawful interference. Express the desire to move forward with the proposed SSGC "Legal" working group at the earliest practical availability.

12 AIA Civil Aviation Cybersecurity Committee Implementation and Go Forward Plan

In summary, assuring the future safety and security of the global aviation system in the face of increasing cyber threats requires an approach that recognizes both the political and technical considerations. Addressing the political considerations requires a plan to align the US stakeholders first and then extend the effort to like-minded nations. To this end, the next steps plan for AIA Civil Aviation Cybersecurity Working Group will include the following:

- Brief the report to the AIA CARS Committee / CAC and then share the recommendations with aviation industry & government stakeholders
- Prioritize recommendations on actions needed to close the identified gaps
- Continue to engage government channels to support and improve the recommendations of this report
- Work with US aviation industry partners and international industry partners via A-ISAC, ASD and ICCAIA to support and improve the recommendations of this report
- Work through ICCAIA to engage ICAO.
- Reach out to the global industry, international governments to gain support and then to build and implements harmonized plans to address the improved recommendations

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

Appendix A: Members & Contributors

AIA Cybersecurity Committee Members:

David Almeida	*LS Technologies*	Daniel Prince	*GE Aviation*
Steve Benham	*GE Aviation*	Leslie Riegle	*AIA*
Curt Bisterfeldt	*GE Aviation*	James Robinson	*Boeing*
Britton, Stephanie	*Bell*	Stefan Schwindt	*GE Aviation*
Cláudio Henrique de Castro	*Embraer*	Jason Shuler	*Astronautics*
Diana Cooper	*Precision Hawk*	Brittany Skelton	*Boeing*
Brian Connolly	*Boeing*	Sean Sullivan	*Boeing*
Dan Diessner	*Boeing*	Wendy Sullivan	*Gulfstream*
Matt Gomez	*Bell*	Ryan Terry	*Lockheed Martin*
Todd Gould	*Boeing*	Jason Timm	*AIA*
John Hoevenher	*Rhinestahl*	Jeff Troy	*GE*
Dave Jones	*Astronautics*	Scott Pepper	*Boeing*
Tom McGoogan	*Boeing*	Mike Vanguardia	*Boeing*
Jennifer Miosi	*GE*	Nina Vajda	*Honeywell*
Patrick Morrissey	*Collins Aerospace*	Keith Wallace	*LS Technologies*
Larry Nace	*Harris*	Brian Witten	*UTC*
Richard Nguyen	*Boeing*	Henry (Hank) Wynsma	*GE Aviation*
Siobvan Nyikos	*Boeing*	Nathan Wright	*Bell*
Eric Ransom	*Bell*		

AIA Cybersecurity Committee Guests/Observers:

Alan Burke	*DoD*	Terry Kirk	*Aviation ISAC*
Gabe Elkin	*MIT Lincoln Labs*	Samantha Lopresti	*FAA*
Will Gonzalez	*FAA*	Steve Ramdeen	*FAA*
Sidd Gejji	*FAA*	Rob Segers	*FAA*
Cesar Gomez	*FAA*	Randy Talley	*ACI*
Jerry Hancock	*Inmarsat/ASD*	Lt Col Eric D. Trias	*USAF*
Luci Holemans	*FAA*	Brian Verna	*FAA*
Ayan Islam	*DHS*	Isidore Venetos	*FAA*
Remzi Seker	*ERAU*		