Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation

Edition 3.0 | December 2021

Table of Contents

Revision Record

Revision Table

Revision	Date	Section(s)	Significant Changes
Edition 3.0	December 2021	All sections.	Third release – content update.
Edition 2.0	April 2021	All sections.	Second release – content update.
Edition 1.1	January 2021	Section 2 and section 4.	Content update and minor adjustments.
Edition 1.0	August 2020		First release.

Purpose

The purpose of this document is to provide an overview of regulations, standards, and guidance related to aviation cyber security. Please note that **this Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation** is a non-exhaustive list. This document will be regularly updated, considering the crucial developments and changes related to aviation cyber security regulations, standards, and guidance.

The list is divided into four following sections:

- International Instruments and Documents;
- Regional and National Regulations and Documents;
- Aviation Industry Cyber Specific Documents; and
- Other Relevant Cyber Industry Framework.

Each section contains the name of the organization/owner of the document, brief description, status, tags, and the URL link to the website where the document is published or available for purchase from the publication owner.

For more information, comments, and suggestions related to this document, or if you represent any of the organizations mentioned in this document and would like to engage with us on aviation cyber security, please contact us at aviationsecurity@iata.org.

1. International Instruments and Documents

This section is specifically related to the international legal instruments like international conventions that refer, indirectly or directly, to cyber security. Moreover, this section is focused on the International Civil Aviation Organization (ICAO) and its documents that address cyber security.

TABLE 1. INTERNATIONAL INSTRUMENTS AND DOCUMENTS

Organization	Regulation / Standard / Recommendation Name	Purpose / Comments / Precis	Status	#Tag	Source
International Air Law Instruments	**Convention for the Suppression of Unlawful Seizure of Aircraft (1970)**	The **Hague Convention of 1970** was adopted in order to combat aircraft hijacking. It contains provisions for the criminalization of offences committed on board an aircraft in flight when a person seizes or exercises control of the aircraft. It needs to be noted that the Hague Convention may apply to aviation cyber security in case a passenger onboard takes control of the aircraft through a cyber-attack.	In Force	#LegalInstrument #Convention #Aircraft	URL Link
	Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)	The **Montreal Convention of 1971** takes an effect-based approach to determine the offences that have the following in common: the acts are unlawful and intentional, and the acts are likely to endanger the safety of aircraft in flight. As per the provisions of the Montreal Convention and its applicability, there is no requirement for the offender to be on board an aircraft at the time of committing the unlawful act. Therefore, this broadens the applicability scope of the Montreal Convention to include any remote cyber-attack affecting not only the aircraft but also air navigation facilities and any providers of critical information that are sent to the aircraft.	In Force	#LegalInstrument #Convention #Transversal	URL Link
	Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful	The Montreal Convention was amended by the **Airport Protocol of 1988** with an aim to extend its catalog of offenses and include any unlawful acts (violence or disruption of services) at international airports. The scope of applicability relative to cyber-attacks is similar as introduced by the Montreal Convention of 1971; however, it is broadened to any cyber-attacks targeting the airport.	In Force	#LegalInstrument #Convention #Aerodromes	URL Link

	Acts against the Safety of Civil Aviation (1971)				
	Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (2010)	The **Beijing Convention of 2010** was introduced with the primary aim to consolidate the scope of the Montreal Convention of 1971 and the Airport Protocol of 1988. However, the Beijing Convention incorporated the broader jurisdiction bases, including the unlawful acts committed in the territory and/or national jurisdiction. The Beijing Convention further expands the applicability scope to the cyber-attacks targeting the air navigation facilities defining them as signals, data, information, or systems necessary for aircraft navigation. Moreover, the Beijing Convention addresses any attacks on such facilities and aircraft conducted by cyber means.	In Force	#LegalInstrument #Convention #Transversal	URL Link
	Beijing Supplementary Protocol to the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010)	The **Beijing Supplementary Protocol of 2010** supplements the Hague Convention of 1970 and broadens the scope of unlawful acts reflecting the development and state of technology that may be used to commit unlawful acts against aviation. For the first time, the legal instrument directly refers to cyber security by including within its scope the seizure of aircraft by any technological means. In order to apply this Protocol, there is no requirement that the offender must be onboard the aircraft during the perpetration of the unlawful act. Therefore, the Beijing Supplementary Protocol of 2010more directly covers cyber-attacks than any other international legal instrument within civil aviation.	In Force	#LegalInstrument #Convention #Aircraft	URL Link
International Civil Aviation Organization (ICAO)	**Annex 17 – Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference**	**Annex 17 (Security) to the Chicago Convention** includes a set of Standards and Recommended Practices (SARPs) relative to aviation security and acts of unlawful interference. The Contracting States to the Chicago Convention are required to develop and implement regulations in order to safeguard civil aviation against acts of unlawful interference. Considering the definition of acts of unlawful interference, it needs to be noted that cyber-attacks may fall within its scope whenever they impact aviation safety.	Published 11th Edition, March 2020	#SARPs #Transversal	URL Link

		Within Annex 17, Standard 4.9.1 (measures relating to cyber threats) has been introduced, which requires States to develop and implement measures to protect their critical information, communications technology systems, as well as data used for civil aviation purposes from unlawful interference.			
	Aviation Cybersecurity Strategy	The ICAO **Aviation Cybersecurity Strategy** has endorsed during the 40th Session of the ICAO Assembly and published in 2019, Considering the multifaceted and multidisciplinary nature of cyber security and noting that cyber-attacks may rapidly affect a wide spectrum of areas, ICAO's works aimed to deliver a common vision and define a set of global principles addressed by the Strategy. The Aviation Cybersecurity Strategy is aligned with other ICAO activities relative to cyber security and coordinated with the safety and security management provisions. The goal of the Strategy will be achieved by the series of principles, measures, and actions addressed through the following seven pillars: • International cooperation; • Governance; • Effective legislation and regulations; • Cybersecurity policy; • Information sharing; • Incident management and emergency planning; and • Capacity building, training, and cybersecurity culture In Q4 of 2020, the ICAO Council adopted the Cybersecurity Action Plan (CyAP) to implement the Cybersecurity Strategy. More information can be found here. The updated version of the ICAO CyAP is expected in early 2022.	Published, October 2019	#Strategy #Transversal	URL Link
	Doc 8973 Aviation Security Manual (Restricted)	The ICAO **Aviation Security Manual (Doc 8973 – Restricted)** aims to assist States with the implementation of Annex 17 by providing guidance, primarily on how to apply SARPs. This document is revised continuously in order to address new threats and technological improvements to prevent acts of unlawful interference.	Published 12th Edition, 2020	#SARPs #Guidance #Transversal	URL Link

	Doc 9985 Air Traffic Management Security Manual (Restricted)	The ICAO **Air Traffic Management Security Manual (Doc 9985 – Restricted)** complements the Aviation Security Manual and provides guidance on security issues relative to air traffic management. This document aims to assist States and Air Traffic System Providers (ATSPs) with implementing the appropriate security provisions in order to meet the requirements of the NCASP. Moreover, this manual provides guidance relative to the ATSP on ATM security services provisions to support national security and law enforcement requirements. It also provides guidance on the protection of the ATM system infrastructure against threats and vulnerabilities.	Published 1st Edition, 2013	#SARPs #Guidance #ATM/ANSP	URL Link
	Doc 10108 Global Risk Context Statement (Restricted)	The **Global Risk Context Statement (Doc 10108 – Restricted)** contains a global aviation security risk assessment, including a global threat picture, and is intended to help inform and support States in national and local aviation security risk assessment processes. Appendix A of this document includes the risk assessment methodology and process map for the global risk assessment and any other guidance to assist States with their national risk assessments.	Published 1st Edition, 2018	#RiskAssessment #Guidance #Transversal	URL Link
	Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation	The **Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation** supersedes Assembly Resolution A39-19. This resolution introduced the ICAO Cybersecurity Strategy as well as instructed ICAO Secretary General to: • develop an action plan to support States and industry in the adoption of the Cyber Security Strategy; and • swiftly conduct a feasibility study and gap analysis for consideration by the Council in order to identify the most appropriate cyber security governance structure and coordinating mechanisms to ensure a multidisciplinary approach to cyber security, and foster sharing of information.	In Force (2019)	#Resolution #Transversal	URL Link

2. Regional and National Regulations and Documents

This section is specifically related to the regional (i.e., the European Union) and national regulations, recommendations, documents including strategy and/or guidance related to aviation cyber security.

TABLE 2. REGIONAL AND NATIONAL REGULATIONS AND DOCUMENTS					
Organization	**Regulation / Standard / Recommendation Name**	**Purpose / Comments / Precis**	**Status**	**#Tag**	**Source (URL Link)**
European Parliament	**Regulation (EU) 2018/1139**	The **Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency**, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91. In 2018, the Council of the European Union adopted a new Basic Regulation on common rules for civil aviation, including the revised mandate for EASA that refers to: • Contributing to the implementation of European Union rules in the area of cyber security; • Ensuring the interdependencies between the different aviation safety domains and aviation safety, cyber security, and other technical domains of aviation regulation are considered and included in any activities.	In Force	#BasicRegulation #CommonRules #Transversal	URL Link
	Regulation (EU) No 376/2014	The **Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis, and follow-up of occurrences in civil aviation**, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007.	In Force	#Regulation #Reporting #Safety #Transversal	URL Link

		This regulation provides rules to improve aviation safety, primarily by ensuring that relevant safety information is reported, collected, stored, protected, exchanged, analyzed, and finally disseminated with follow-up at the industry level. This regulation provides the means to increase information exchange between the Member States and ensures the continued availability of safety information. The Member States, EASA, and organizations, based on this regulation, shall establish a mandatory and voluntary occurrence reporting system that will collect any serious risk event.			
	General Data Protection Regulation (GDPR)	The **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data**, and repealing Directive 95/46/EC**.** This regulation addresses data protection and privacy within the European Union and the European Economic Area. The Regulation also addresses the transfer of data outside the European Union and the European Economic Area.	In Force	#Regulation #DataProtection #GDPR #Transversal	URL Link
	Directive (EU) 2016/1148 (NIS Directive)	The **Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union**. The Directive established the European competence for cyber security in order to protect the security of network and information systems by addressing three main objectives: • Improving national cybersecurity capabilities (having a common and minimum baseline set of capabilities); • Facilitating the cross-border cooperation between the Member States and the European Union (strategic/policy as well as operational cybersecurity levels); and • Promoting a culture of risk management and incident reporting. Currently, there are ongoing works on the **NIS 2.0 Directive** proposal. More information can be found here.	In Force	#Directive #NetworkSecurity #InformationSystems #Transversal	URL Link

European Commission	**Implementing Regulation (EU) 2015/1998**	The **Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security**. The Regulation provides detailed measures for implementing the common basic standards to safeguard civil aviation against acts of unlawful interference that jeopardize civil aviation security and acts of unlawful interference posed by cyber threats. This regulation is in force; however, it will be amended by the Regulation (EU) 2019/1583.	In Force	#Regulation #SecurityMeasures #Transversal	URL Link
	Implementing Regulation (EU) 2019/1583	The **Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures**. This amendment introduces detailed measures for implementing the common basic standards on aviation security regarding cyber security measures.	Date of entry into force unknown, Date of effect: 31/12/2021	#Regulation #SecurityMeasures #Transversal	URL Link
	Implementing Regulation (EU) 2017/373	The **Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight**, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011. This regulation introduced requirements for Air Traffic Management/Air Navigation Services Providers as well as other air traffic management network functions and their oversight.	In Force	#Regulation #SecurityMeasures #ATM/ANSP	URL Link
	Transport Cybersecurity Toolkit	The European Commission published the **Transport Cybersecurity Toolkit**, providing tips and recommendations for enhancing cyber security awareness and resiliency within the transport industry, including aviation.	Published, December 2020	#Recommendations #Toolkit #Transversal	URL Link

European Aviation Safety Agency (EASA)	**EASA RMT.0648 – Aircraft Cybersecurity**	The rule **RMT.0648 – Aircraft Cybersecurity** relates to the mitigation of the safety effects stemming from cyber risks (i.e., acts of unlawful interference against the electronic networks and systems of the aircraft). The key objective of this rule is to mitigate the safety effects coming from cyber risks due to acts of unlawful interference against the networks and information systems onboard aircraft. These Acceptable Means of Compliance (AMC) addresses cyber security provisions taking into account the existing special condition and recommendations of the FAA ASISP ARAC group. The **ED Decision 2020/006/R** issued amendments to different Certification Specifications (CS), e.g., CS-25 (large aircraft) and the related acceptable means of compliance (AMC) and/or guidance material (GM), together with the AMC/GM to Part 21 (**Certification of aircraft and related products, parts and appliances, and of design and production organizations),** is the Annex to the Commission Regulation (EU) No 748/2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organizations.	Decision made on 24/06/2020, in force.	#AMC #NetworkSecurity #InformationSystem #Security #Aircraft	URL Link URL Link
	EASA RMT.0720 – Management of Information Security Risks	The rule **EASA RMT.0720 – Management of Information Security Risks** will introduce provisions for the cyber security risks management by organizations (i.e., design, production, continuing airworthiness management, maintenance, operations, aircrew, ATM/ANS, aerodromes). The main objective is to efficiently contribute to protecting the aviation system from cyber security attacks and their consequences. It is proposed to introduce provisions in all the aviation domains (design, production, continuing airworthiness management, maintenance, operations, aircrew, ATM/ANS, aerodromes) to achieve this objective. Affected rules: Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011, and No 965/2012 and related AMC and GM.	Ongoing work, EASA Opinion issued in June 2021.	#AMC #RiskManagement #InformationSecurity #Transversal	URL Link URL Link

European Civil Aviation Conference (ECAC)	**ECAC Doc 30, Part II (Restricted)**	The **ECAC Doc 30, Part II Chapter 14,** delivers recommendations relative to cyber security governance at the national level and addresses activities at the organizational level. It represents a risk-based approach. The recommendations implemented at the national level need to be implemented and followed by operators or other stakeholders (i.e., service providers, air navigation service providers, airport operators, aircraft operators, regulated agents, etc.) using a critical infrastructure. The main aim of this document and its recommendations is to ensure safe and secure aviation operations by applying processes and procedures to maintain the confidentiality, integrity, and availability (CIA) of the systems and data.	In Force	#Recommendation #Governance #Transversal	URL Link
European Strategic Coordination Platform (ESCP)	**Strategy for Cyber Security in Aviation (2019)**	The ESCP published the **Strategy for Cyber Security in Aviation (2019)** as the First Issue in September 2019. This Strategy was adopted by the ESCP before the 40th Session of the ICAO General Assembly with the acknowledgment that it will be revised to ensure consistency with the ICAO Aviation Cybersecurity Strategy.	Published, September 2019	#Strategy #Transversal	URL Link
United States: **Federal Aviation Administration (FAA)**	**Code of Federal Regulations (CFR) Title 14 Aeronautics and Space (incl. Part 23, 25, 27, 29, etc.)**	The **Code of Federal Aviation Regulations** introduces rules prescribed by the Federal Aviation Administration (FAA) to govern all aviation activities. The FARs are part of Title 14 of the Code of Federal Regulations (CFR), addressing a broad spectrum of aviation activities, including inter alia aircraft design and maintenance, airline flights, pilot training, model aircraft operations, as well as Unmanned Aircraft Systems (UAS). This regulation aims to promote safe aviation, protect the crew, passengers, and the general public from unnecessary risk.	In Force	#LegalInstrument #Transversal	URL Link
	FAA Reauthorization Act of 2018, Public Law No: 115-254	The **FAA Reauthorization Act of 2018** sets provisions regarding unmanned aircraft systems (UAS), cyber security, and any FAA activities in these terms.	In Force	#LegalInstrument #Transversal	URL Link
	Flight Standards Information Management System (FSIMS)	The **Flight Standards Information Management System (FSIMS)** is the FAA order that addresses the provisions related to the activities of aviation safety inspectors (ASI) responsible for the:	In Force	#LegalInstrument #Transversal	URL Link

		• certification; • technical administration; and • surveillance of air carriers and other air operators performing operations according to the appropriate part of **Title 14 of the Code of Federal Regulations (14 CFR)**, certificated airmen, and other aviation activities.			
	Advisory Circular 119-1 - Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)	This **Advisory Circular (AC) Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP) i**ntroduces the acceptable means of compliance in the process to obtain operational authorization for a certified aircraft in terms of special conditions relative to the onboard computer network. NOTE: This Advisory Circular is not mandatory; it does not constitute a regulation. However, if used, you must conform to it in totality.	Issued, September 2015	#AdvisoryCircular #Airworthiness #Aircraft #NetworkSecurity	URL Link
	Policy PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security	This policy statement, **Establishment of Special Conditions for Cyber Security,** provides the guidance directed to the Aircraft Certification Offices for the application of special conditions in order to address cyber security vulnerabilities in aircraft certification programs.	Issued, March 2014	#Policy #Aircraft #Certification #Transversal	URL Link
United States: **Transportation Security Administration (TSA)**	**TSA Cybersecurity Roadmap**	The TSA Cybersecurity Roadmap discusses four priorities and six goals on cyber security in order to improve the protection of information technology systems, which are aligned with the National Cyber Strategy and the Department of Homeland Security (DHS) Cybersecurity Strategy.	Published, November 2018	#Roadmap #Transversal	URL Link
United Kingdom: **Civil Aviation Authority (CAA)**	**Aviation Cyber Security Strategy**	The **Aviation Cyber Security Strategy** provides the aviation industry with a clear timeline for cyber security up to 2021/22. This document complements the National Cyber Security Strategy and 2050 Aviation Strategy. Key objectives of the Strategy: • Understating the risk posed by cyber threats and existing vulnerabilities, and analyzing the consequences; • Managing cyber risks - take actions that are appropriate and proportionate;	Published, July 2018	#Strategy #Transversal	URL Link

		• Responding and recovering from cyber-attacks; and • Promoting cultural change, increasing capabilities, and raising awareness.			
	CAP1850: Cyber Assessment Framework (CAF) for Aviation	The **Cyber Assessment Framework (CAF) for Aviation** is the scalable and proportionate oversight tool developed by the UK CAA, aiming to help with cyber security posture assessment within the aviation organization.	Published, August 2020	#CyberPosture #Assessment #Transversal	URL Link
	CAP1753: CAA Cyber Security Oversight Process for Aviation	The **Cyber Security Oversight Process for Aviation** provides the basis for cyber security oversight activity by the UK CAA. This oversight process also provides details on a good cyber security practice.	Published, August 2020	#OversightProcess #Transversal	URL Link
Qatar: **Civil Aviation Authority (CAA)**	**Aviation Cyber Security Guidelines**	The **Aviation Cyber Security Guidelines**, developed by the Qatar CAA, provide standards and principles relative to securing the critical aviation systems and the best practices relative to electronic security. These guidelines aim to assist the industry in improving cyber security posture and building resiliency within the organization. The scope of this document is focused inter alia on the following: • Air Traffic Control Systems • Airport Operators • Airport Information Systems • Aircraft operators • Aircraft Systems • Airport Tenants (e.g., QAS Cargo, QACC, QDF, etc.). The guidelines document is directed to the following stakeholders managing the critical information systems within the aviation ecosystem: • Air Traffic Control operators managing communication with aircraft; • Airport Authorities / Operators managing critical information systems at airports (i.e.., Passenger Information Systems, Airport Information System, Baggage Handling systems, etc.); • Information Systems within an aircraft (communication systems, flight entertainment systems, internal controls, etc.).	Published, June 2019	#Guidance #Transversal	URL Link

Singapore: **Civil Aviation Authority of Singapore (CAAS)**	**Advisory Circular (AC) 121-7-2, Aircraft Network Security Programme (ANSP)**	This Advisory Circular on the **Aircraft Network Security Programme (ANSP)** provides guidance in order to demonstrate compliance with, and information related to, requirements of the Air Operator Certificate (AOC) holder relative to managing aircraft network security program as part of continuous airworthiness. This AC is applicable to an AOC holder operating an aircraft specified by the aircraft manufacturer to require an ANSP. An aircraft requiring an ANSP to operate can be identified by a Special Condition (SC) listed on the Type Certificate Data Sheet (TCDS) or, if later modified, will be identified in the Supplemental Type Certificate (STC) or Amended Type Certificate (ATC) with the SC.	Issued, September 2018	#AdvisoryCircular #Airworthiness #Aircraft #NetworkSecurity	URL Link

3. Aviation Industry Cyber Specific Documents

This section is specifically related to the aviation industry cyber-specific documents, including guidance, toolkits, standards, etc.

TABLE 3. AVIATION INDUSTRY CYBER SPECIFIC DOCUMENTS

Organization	Regulation / Standard / Recommendation Name	Purpose / Comments / Precis	Status	#Tag	Source (URL Link)
International Air Transport Association (IATA)	**IOSA Standards Manual (ISM) 14th Edition,**	The **IOSA Standards Manual (ISM)** is published in order to provide the IOSA standards, recommended practices (ISARPs), associated guidance material, and other supporting information necessary for an operator to prepare for an audit successfully. The Edition 14th includes: • New recommended practice and guidance derived from Annex 17; addresses the identification and protection from unlawful interference of critical operational information and communications technology systems and data used in or in support of operations (alignment with Annex 17). • Extensive revision to add cybersecurity to security threats that must be subjected to risk assessment and mitigation (alignment with Annex 17).	Published, December 2020 Effective: September 2021	#Standard #Recommendation #GuidanceMaterial	URL Link
	Security Management System (SeMS) Manual, Edition 5	The **Security Management System (SeMS)** Manual is the all-encompassing guidance material (including aviation cyber security) to assist entities in building effective aviation security measures through a standardized structure.	Published, November 2021	#Guidance #Transversal	URL Link
	Aviation Cyber Security Guidance Material, Edition 1	This Aviation Cyber Security Guidance Material, developed with our airline members, details recommendations on adopting a minimal cyber security posture. • Part 1: Organization Culture and Posture relates to the cyber security of the organization; • Part 2: Aircraft relates to the cyber security of the aircraft and risk management.	Published, February 2021	#Guidance #Organization #Aircraft	URL Link

		Please note that this guidance material will be continuously updated.			
Civil Air Navigation Services Organization (CANSO)	**Standard of Excellence in Cybersecurity**	The **Standard of Excellence in Cybersecurity** provides set of best practices and guidance from aviation industry stakeholders in order to assess and improve the ANSP's cyber security performance and their supply chain. This document aims to assist the CISOs and security mangers in assessment of the cyber security maturity and exposure to risks.	Published, September 2020	#BestPractices #Guidance #ANSP #ATM	URL Link
	Air Traffic Management Cybersecurity Policy Template	The **Air Traffic Management Cybersecurity Policy Template**, developed by CANSO, ICAO, and Airbus, aims to assist the states with implementation of the cyber security mechanisms and culture for the ATM systems.	Published, March 2021	#Policy #Template #ATM	URL Link
Airports Council International (ACI)	**Cybersecurity for Airport Executives Handbook**	The **Cybersecurity for Airport Executives Handbook** is directed to airport executives as well as senior airport management. It provides guidance relative to cyber security management.	Published, 2019	#Guidance #Aerodromes	URL Link
	Cybersecurity Implementation Handbook	The **Cybersecurity Implementation Handbook** is directed to the airport operators with an aim to help understand best practices for addressing cyber security threats. It provides guidance from the stage of cyber security framework implementation to the stage of technical strategies.	Published, 2020	#Guidance #Aerodromes	URL Link
European Organisation for Civil Aviation Equipment (EUROCAE)	**ED-201 - Aeronautical Information System Security (AISS) Framework Guidance**	The **ED-201 - Aeronautical Information System Security (AISS) Framework Guidance** focuses on the shared responsibility for the AISS. This responsibility is shared between all stakeholders being part of the aviation ecosystem. This document aims to help ensure the safety of the flight and maintain the operation of the aviation infrastructure without major disruptions. The scope of this guidance covers the design of aircraft, its production, operations, ATM, aerodromes, maintenance, aviation service providers, components and information, and the supply chains. Currently, there are ongoing works on the ED-201A.	Issued, December 2015 Ongoing works on the update (ED-201A)	#Guidance #AISS #Transversal	URL Link
	ED-202A - Airworthiness Security Process Specification	The **ED-202A - Airworthiness Security Process Specification** provides additional guidance for aircraft certification for handling cyber threats to aircraft safety.	Issued, June 2014	#Guidance #Airworthiness	URL Link.

		The ED-202A introduced the requirements and compliance objectives for aircraft development and certification. This guidance should be used with the following guidance: ED-79A / SAE ARP4754A, ED-12C / DO-178C, and ED-80 / DO-254, as well as with the advisory material associated with the following: FAA AMJ25.1309, and EASA AMC25.1309, in the context of Part 25, CS-25, and JAA JAR- 25. The ED-202A was designed for the Original Equipment Manufacturers (OEMs) and any entity applying for an initial Type Certificate (TC), Design Approval Holders (DAH), Supplemental Type Certificate (STC), and Amended Type Certificate (ATC) or changes to TC for installation and continued airworthiness for aircraft systems.		#Design #AircraftCertification #OEM #Aircraft	
	ED-203A - Airworthiness Security Methods and Considerations	The **ED-203A - Airworthiness Security Methods and Considerations** provides guidance to protect the airworthiness of the aircraft from intentional unauthorized electronic interaction. This guidance provides methods and considerations to help prove compliance for airworthiness security during the entire lifecycle of aircraft. The ED-203A provides guidance to accomplish the airworthiness security process activities defined in the ED-202A / DO-326A.	Issued, June 2018	#Guidance #Airworthiness #Security #Aircraft	URL Link
	ED-204A - Information Security Guidance for Continuing Airworthiness	The **ED-204A - Information Security Guidance for Continuing Airworthiness** provides guidance relative to the following stages of the product lifecycle: operation, support, maintenance, administration, and deconstruction. The ED-204A provides guidance relative to information security risks. What is important, the security measures provided with this guidance are not limited to mitigate only the information technology risks but also physical or organizational.	Issued, September 2020	#Guidance #ContinuousAirworthiness #Security #Aircraft	URL Link
	ED-205 - Process Standard for Security Certification and Declaration of ATM ANS Ground Systems	The **ED-205 - Process Standard for Security Certification and Declaration of ATM ANS Ground Systems** provides guidance on the process to assess the extent of security of the ATM/ANS ground systems. This process can be used to	Issued, March 2019	#Standards #Guidance #SecurityCertification #ATM/ANSP	URL Link

		identify, evaluate, and manage impacts on safety, operational delivery, and other commercial concerns. The ED-205 provides standards for certification or declaration of conformity with security requirements. Currently, there are ongoing works on the ED-205A.			
	ED-206 – Guidance on Information Security Event Management	The **Information Security Event Management (ISMS)** is currently in draft. Joint activity with the RTCA DO-392.	Ongoing (to be issued in 2022)	#Guidance #EventManagement #Transversal	N/A
EUROCONTROL	**ATM Cyber Security Maturity Model**	The **Cyber Security Maturity Model** describes a range of capabilities to be adopted in the organization for an effective approach to cybersecurity. This document provides a description of the kinds of activities and processes at different levels of maturity.	Published, September 2019	#Guidance #MaturityModel #ATM/ANSP	URL Link
	Monitoring Cyber Security Events – EATM-CERT Interactive Map	**EUROCONTROL/EATM-CERT** produced an interactive world map of publicly reported cyber events impacting aviation.	Published	#CybersecurityEvent #Map #Transversal	URL Link
RTCA	**DO-178C, Software Considerations in Airborne Systems and Equipment Certification**	The **DO-178C, Software Considerations in Airborne Systems and Equipment Certification,** introduces recommendations for software production for airborne systems and equipment that performs its intended function with a level of confidence in safety in compliance with the airworthiness requirements.	Issued, December 2011	#Guidance #AirborneSystems #EquipmentCertification	URL Link
	DO-326A, Airworthiness Security Process Specification	The **DO-326A, Airworthiness Security Process Specification provides** additional guidance for aircraft certification for handling cyber threats to aircraft safety. The DO-326A introduced the requirements and compliance objectives for aircraft development and certification. This guidance should be used with the following guidance: ED-79A / SAE ARP4754A, ED-12C / DO-178C, and ED-80 / DO-254, as well as with the advisory material associated with the following: FAA AMJ25.1309, and EASA AMC25.1309, in the context of Part 25, CS-25, and JAA JAR- 25. This DO document was designed for the Original Equipment Manufacturers (OEMs) and any entity applying for an initial Type Certificate (TC), Design Approval Holders (DAH), Supplemental Type Certificate (STC), and Amended Type Certificate (ATC) or	Issued, August 2014	#Guidance #Airworthiness #Security #Aircraft	URL Link

		changes to TC for installation and continued airworthiness for aircraft systems.			
	DO-355A - Information Security Guidance for Continuing Airworthiness	The **DO-355A - Information Security Guidance for Continuing Airworthiness** provides guidance relative to the following stages of the product lifecycle: operation, support, maintenance, administration, and deconstruction. The DO-355A provides guidance relative to information security risks. What is important, the security measures provided with this guidance are not limited to mitigate only the information technology risks, but also physical or organizational.	Issued, September 2020	#Guidance #ContinuousAirworthiness #Security #Aircraft	URL Link
	DO-356A - Airworthiness Security Methods and Considerations	The **DO-356A - Airworthiness Security Methods and Considerations** provides guidance to protect the airworthiness of the aircraft from intentional unauthorized electronic interaction. This guidance provides methods and considerations to help prove compliance for airworthiness security during the entire lifecycle of aircraft. The DO-356A provides guidance to accomplish the airworthiness security process activities defined in the ED-202A / DO-326A.	Issued, June 2018	#Guidance #Airworthiness #Design #AircraftCertification #OEM #Aircraft	URL Link
	DO-392 - Guidance on Information Security Event Management	The **Guidance on Information Security Event Management (ISMS)** is currently in draft. Joint activity with the EUROCAE ED-206.	Ongoing (to be published in 2022)	#Guidance #EventManagement #Transversal	N/A
Aeronautical Radio, Incorporated (ARINC)	**ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework**	The **ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework** provides information in order to facilitate the understanding of aircraft information security as well as to information to help the development of aircraft information security operational concepts. The ARINC Report 811 also provides information on the aircraft information security process framework for aircraft operators according to their needs. This document, once implemented, aims to enable the safe and secure dispatch of the aircraft on time. Moreover, the framework represents the development of aircraft information security that is cost-effective, also	Published, December 2005	#Report #Framework #InformationSecurity #Aircraft	URL Link

		providing a common language in terms of understanding the security needs.			
	ARINC Specification 823P1 DataLink Security, Part 1 - ACARS Message Security	The **ARINC Specification 823P1 DataLink Security, Part 1 - ACARS Message Security** provides standards for ACARS Message Security (AMS) that permits the exchange of ACARS datalink messages, in a secure, authenticated manner by using a uniform security framework, between aircraft and ground systems. The security framework introduced by the ARINC Specification 823P1 is based on open international standards. These standards are compliant with the ACARS datalink communications environment.	Published, December 2007	#Standard # DataLink_Security # ACARS #Aircraft #GroundSystems	URL Link
	ARINC Specification 823P2 DataLink Security, Part 2 - Key Management	The **ARINC Specification 823P2 DataLink Security, Part 2 - Key Management** provides recommendations for the ACARS Message Security (AMS) key management. The key management framework introduced by the **ARINC Specification 823P2** is based on open international standards. These standards are compliant with the ACARS datalink communications.	Published, March 2008	#Standard # DataLink_Security # KeyManagement #Aircraft #Ground_Systems	URL Link
	ARINC Specification 834-8 Aircraft Data Interface Function (ADIF)	The **ARINC Specification 834-8 Aircraft Data Interface Function (ADIF)** provides information on the ADIF for aircraft installations incorporating network components based on the available commercial technologies. The ARINC Specification 834-8 introduces a set of protocols and services in terms of the exchange of aircraft avionics data across aircraft networks. This document aims to have a common set of services for the access of specific avionics parameters.	Published, July 2020	#Standard #ADIF #Aircraft	URL Link
	ARINC Report 835-1 Guidance for Security of Loadble Software Parts Using Digital Signatures	The **ARINC Report 835-1** provides background and detailed technical information relative to the existing methods in order to secure loadable software parts.	Published, January 2014	#Guidance #LoadbleSoftware #DigitalSignatures #Aircraft	URL Link
	ARINC 858P1 Internet Protocol Suite (IPS) for Aeronautical Safety	The **ARINC 858P1**document with technical requirements and standards for airborne ATN/IPS systems. ATN/IPS aims to improve aviation safety communication services.	Published, June 2021	#Guidance #ATN/IPS	URL Link

	Services, Part 1, Technical Requirements				
	ARINC Report 852 Guidance for Security Event Logging in an IP Environment	The **ARINC Report 852 Guidance for Security Event Logging in an IP Environment** provides the guidance for IP-based onboard networks and systems in the following aircraft domains: The Airline Information Services (AIS) and Passenger Information Entertainment Services (PIES). The ARINC Report 852 introduces a common set of security-related data elements and format(s) produced by aircraft systems.	Published, June 2017	#Guidance #LoadbleSoftware #DigitalSignatures #Aircraft	URL Link
	ARINC Report 658 Internet Protocol Suite (IPS) for Aeronautical Safety Services - Roadmap Document	The **ARINC Report 658 Internet Protocol Suite (IPS) for Aeronautical Safety Services - Roadmap Document** provides information on the expanding role of data communication technology as well as its evolution moving from ACARS protocols to ATN/OSI protocols, and finally ATN/IPS protocols with secure networks. The standards related to the ATN/IPS are coordinated with other international standards organizations (i.e., ICAO, EUROCAE, and RTCA).	Published, December 2017	#Guidance #IPS #ATN/OSI #ATN/IPS #Aircraft	URL Link
	ARINC Specification 664P1-2 Aircraft Data Network, Part 1, Systems Concepts and Overview	The **ARINC Specification 664P1-2 Aircraft Data Network, Part 1**, Systems Concepts and Overview provides standards on the data networking used in commercial aircraft installations. The ARINC Specification 664P1-2 provides information on how to adapt commercially defined networking standards to an aircraft environment.	Published, June 2019	#Standard #DataNetwork #Aircraft	URL Link
A4A (Airline for America, former ATA)	**ATA Spec 42 Aviation Industry Standards for Digital Information Security**	The **ATA Spec 42 Aviation Industry Standards for Digital Information Security delivers recommendations** on standardized methods to achieve an appropriate security level for the applications that rely on digital identities. This document aims to provide guidance to a different variety of stakeholders with security requirements.	Published, latest revision 2020	#Standard #DigitalInformation #Transversal	URL Link
European Standards (EN)	**BS EN 16495:2019 Air Traffic Management. Information security for**	The **BS EN 16495:2019 Air Traffic Management. Information security for organizations supporting civil aviation operations** provides guidance based on the EN ISO/IEC	Published, July 2019	#Standard #InformationSecurity	URL Link

	organizations supporting civil aviation operations	27002:2017 applicable to the organizations that support civil aviation, focusing on ATM operations.		#ATM/ANSP #Transversal	
Original Equipment Manufacturers (OEMs)	**Aircraft Security Guidance and Handbooks, Maintenance Manuals**	Each OEM provides guidance material upon delivery with methods and specifications for the aircraft's security and network.	N/A	#Aircraft #Security	N/A
Multiple Organizations	**Open Architecture for Airport Security Systems, 1st Edition**	This document, prepared by Heathrow Airport Limited and Avinor AS, provides the guidance on the open architecture and the airport security systems. It was endorsed by the following organizations: ACI EUROPE, US Transportation Security Administration, UK Department for Transport, UK Civil Aviation Authority, Canadian Air Transport Security Authority, German Federal Police, Heathrow Airport Limited, Swedavia Airports, Avinor AS, Amsterdam Schiphol Airport, Groupe ADP, Manchester Airport Group, Geneva Airport, Dublin Airport Authority, Birmingham Airport, AVSEC New Zealand, Copenhagen Airports A/S, Munich Airport, Dubai Airports, Changi Airport.	Published, July 2020	#Airport #OpenArchitecture #SecuritySystems	URL Link

4. Other Relevant Cyber Industry Framework

This section is specifically related to the other relevant cyber industry framework, like ISO, NIST, etc., that are also applicable to civil aviation.

TABLE 4. OTHER RELEVANT CYBER INDUSTRY FRAMEWORK

Organization	Regulation / Standard / Recommendation Name	Purpose/Comments/Precis	Status	#Tag	Source
International Organization for Standardization (ISO)	**ISO/IEC/IEEE 15288:2015 Systems and software engineering—Systems life cycle processes**	The **ISO/IEC/IEEE 15288:2015 Systems and software engineering—Systems life cycle processes,** provides a common framework of process descriptions to describe the life cycle of systems. The standards of ISO/IEC/IEEE 15288:2015 define a set of processes and associated terminology from an engineering viewpoint, which can be applied at any level of a system's structure. Some of the processes can be used throughout the life cycle in order to manage and perform the stages of a system's life cycle.	Published, May 2015	#Standard #LifeCycle #Transversal	URL Link
	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	The **ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements** provides a model to facilitate the process of establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system. The standards of ISO/IEC 27001:2013 represent a top-down, risk-based approach as well as technology-neutral and define six stages of the planning process that includes: • Defining a security policy; • Defining the scope of ISMS; • Conducting a risk assessment; • Managing identified risks; • Selecting control objectives and controls for implementation; and • Preparing a statement of applicability.	Published, October 2013	#Standard #IT #SecurityTechniques #SecurityManagement #Transversal	URL Link

	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls	The **ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls** provides guidance on the organization's information security standards and information security management practices. This includes the selection, implementation, and management of controls. The ISO/IEC 27002:2013 document should be used by the organizations that intend to implement ISMS based on the ISO/IEC 27001, implement commonly accepted information security controls, as well as develop information security management own guidance.	Published, October 2013	#Standard #IT #SecurityTechniques #SecurityControls #Transversal	URL Link
	ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management	The **ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management** was developed to support the concepts defined in ISO/IEC 27001 and aims to assist with the implementation of information security that is based on a risk management approach. The standards of ISO/IEC 27005:2018can be applied by different types of organizations to manage risks that can compromise the organization's information security.	Published, July 2018	#Standard #IT #SecurityTechniques #RiskManagement #Transversal	URL Link
	ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts	The **ISO/IEC 27036-1:2014** outlines some standards and guidance on the information and information systems security in terms of supply chain relationships.	Published, April 2014	#Standard #Guidance #SupplierRelationships #Transversal	URL Link
	ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements	The **ISO/IEC 27036-2:2014** outlines requirements on the information and information systems security in terms of supply chain relationships.	Published, August 2014	#Standard #Requirements #SupplierRelationships #Transversal	URL Link
	ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships —	The **ISO/IEC 27036-3:2013** provides guidance on the information and communication technology supply chain security.	Published, November 2013	#Standard #Guidance #SupplierRelationships #Transversal	URL Link

	Part 3: Guidelines for information and communication technology supply chain security				
International Society of Automation	**ISA/IEC 62443-2-1-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program**	The **ISA/IEC 62443-2-1-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program** provides standards for the cyber security management system to be used in the industrial automation and control systems environment.	Published, 2009	#Standard #SecurityProgram #ControlSystems #Transversal	URL Link
	ISA/IEC 62443-3-3-2013 Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels	The **ISA/IEC 62443-3-3:2013 Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels** provides standards on detailed technical control system requirements (SRs) that are associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 (99.01.01)	Published, 2013	#Standard #Requirements #SecurityLevels #Transversal	URL Link
	ISA/IEC-62443-4-2-2018 Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components	The **ISA/IEC-62443-4-2 Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components** provides standards relative to the technical control system component requirements (CRs) that are associated with the seven foundational requirements (FRs) described in ISA-62443-1-1.	Published, 2018	#Standard #Requirements #IACSComponents #Transversal	URL Link
National Institute of Standards and Technology (NIST)	**NIST Framework for Improving Critical Infrastructure Cyber Security Version 1.1**	The **NIST Framework for Improving Critical Infrastructure Cyber Security** introduces information on the voluntary risk management framework that includes: • standards; • guidelines; and • best practices to manage cybersecurity-related risk. The NIST framework is a prioritized, flexible, and cost-effective approach to help to promote the protection and resilience of critical infrastructure.	Published, April 2018	#Standard #Framework #CriticalInfrastructure #Transversal	URL Link
	NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations—A System Life Cycle	The **NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy** describes the Risk Management Framework (RMF). It also provides guidance on how to apply RMF to information systems and organizations,	Published, December 2018	#Standard #RMF #InformationSystem	URL Link

	Approach for Security and Privacy	representing a disciplined, structured, as well as a flexible process for managing security and privacy risk. The described process includes: • information security categorization; • control selection, implementation, and assessment; • system and common control authorizations; and • continuous monitoring.		#LifeCycle #Security&Privacy #Transversal	
	NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View	The **NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View** provides guidance on the integrated, organization-wide program in order to manage information security risk to operations, assets, individuals of the organization, other organizations, as well as the Nation that results from the operation and use of federal information systems.	Published, March 2011	#Standard #InformationSecurity #RiskManagement #Transversal	URL Link
	NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations	The **NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations** delivers a set of security and privacy controls for information systems and organizations with the purpose of protecting organizational operations and assets, individuals, other organizations, as well as the Nation from a diverse set of threats and risks.	Published, September 2020	#Standard #SecurityControls #PrivacyControls #Transversal	URL Link
	NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security	The **NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security** provides guidance relative to the securing of Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), as well as other control system configurations.	Published, May 2015	#Standard #ICS #Transversal	URL Link
	NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	The **NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems** provides guidance from the engineering-driven perspective as well as actions that are necessary for the development of more secure and survivable systems.	Published, November 2016	#Standard #SecurityEngineering #Transversal	URL Link

	NIST SP 800-160 Vol. 2 Rev 1 Developing Cyber Resilient Systems: A Systems Security Engineering Approach	The **NIST SP 800-160 Vol. 2 Developing Cyber Resilient Systems: A Systems Security Engineering Approach** should be used in conjunction with ISO/IEC/IEEE 15288:2015, NIST Special Publication 800-160, Volume 1, and NIST Special Publication 800-37. It contains guidance on the process to achieve the identified cyber resiliency outcomes that are based on the systems engineering perspective and system life cycle processes as well as with risk management processes.	Published, December 2019	#Standard #SecurityEngineering #CyberResiliency #Transversal	URL Link
	NIST SP 1900-202 Cyber-Physical Systems and Internet of Thing	The **NIST SP 1900-202 Cyber-Physical Systems and Internet of Things** provides details on the relationship between the phrases Cyber-Physical Systems (CPS) and the Internet of Things (IoT) and much more.	Published, March 2019	#Standard #CPS #IoT #Transversal	URL Link
	NIST IR 8259 Recommendations for IoT Device Manufacturers	The **NIST IR 8259 Recommendations for IoT Device Manufacturers** provides information on the recommended activities related to cyber security for manufacturers to be performed before the IoT devices are delivered to the customers.	Published, May 2020	#Recommendation #IoT #DeviceManufacturers	URL Link
	NIST IR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	The **NIST IR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry** document provides set of best practices for the cyber supply chain risk management.	Published, February 2021	#BestPractices #SupplyChain #RiskManagement	URL Link
United Nations (UN)	**UN Security Council Resolution 2341**	The **UN Security Council Resolution 2341** recognizes and addresses the growing importance of ensuring the reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security.	Published, 2017	#Resolution #Transversal	URL Link
	Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices	The **Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices** is deliverable from a joint initiative of the following institutions: the UN Office of Counter-Terrorism, the UN Security Council Counter-Terrorism Committee Executive Directorate, and INTERPOL. This compendium provides the Member States and IROs with the guidelines and good practices to protect critical infrastructure from terrorist attacks, including cyber aspects.	Published, June 2018	#Guidance #Transversal	URL Link

Index

1. International Instruments and Documents

International Air Law Instruments

- Convention for the Suppression of Unlawful Seizure of Aircraft (1970)
- Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)
- Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)
- Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (2010)
- Beijing Supplementary Protocol to the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010)

International Civil Aviation Organization (ICAO)

- Annex 17 – Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference
- ICAO Aviation Cybersecurity Strategy
- Doc 8973 Aviation Security Manual (Restricted)
- Doc 9985 Air Traffic Management Security Manual (Restricted)
- Doc 10108 Global Risk Context Statement (Restricted)
- Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation

2. European Regulations and Documents

European Parliament

- Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91
- Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis, and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

European Commission

- Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security
- Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures
- Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011
- Transport Cybersecurity Toolkit

European Aviation Safety Agency (EASA)

- EASA RMT.0648 – Aircraft Cybersecurity
- EASA RMT.0720 – Management of Information Security Risks

European Strategic Coordination Platform (ESCP)

- Strategy for Cyber Security in Aviation

European Civil Aviation Conference (ECAC)

- ECAC Doc 30, Part II (Restricted)

United States: Federal Aviation Administration (FAA)

- Code of Federal Regulations (CFR) Title 14 Aeronautics and Space (incl. Part 23, 25, 27, 29, etc.)
- FAA Reauthorization Act of 2018, Public Law No: 115-254
- Flight Standards Information Management System (FSIMS)
- Advisory Circular 119-1 - Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)
- Policy PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security

United States: Federal Aviation Administration (FAA)

- TSA Cybersecurity Roadmap

United Kingdom (Civil Aviation Authority)

- Aviation Cyber Security Strategy
- CAP1850: Cyber Assessment Framework (CAF) for Aviation
- CAP1753: CAA Cyber Security Oversight Process for Aviation

Qatar (Civil Aviation Authority)

- Aviation Cyber Security Guidelines

Singapore (Civil Aviation Authority of Singapore)

- Advisory Circular (AC) 121-7-2, Aircraft Network Security Programme (ANSP)

3. Aviation Industry Cyber Specific Documents

International Air Transport Association (IATA)

- IOSA Standards Manual (ISM), Edition 14th
- Security Management System (SeMS) Manual, Edition 5
- Aviation Cyber Security Guidance Material, Edition 1

Civil Air Navigation Services Organization (CANSO)

- Standard of Excellence in Cybersecurity
- Air Traffic Management Cybersecurity Policy Template

Airports Council International (ACI)

- Cybersecurity for Airport Executives Handbook
- Cybersecurity Implementation Handbook

European Organisation for Civil Aviation Equipment (EUROCAE)

- ED-201 – Aeronautical Information System Security (AISS) Framework Guidance
- ED-202A – Airworthiness Security Process Specification
- ED-203A – Airworthiness Security Methods and Considerations
- ED-204A – Information Security Guidance for Continuing Airworthiness
- ED-205 – Process Standard for Security Certification and Declaration of ATM ANS Ground Systems
- ED-ISEM – Guidance on Information Security Event Management

EUROCONTROL

- ATM Cyber Security Maturity Model
- Monitoring Cyber Security Events – EATM-CERT Interactive Map

RTCA

- DO-178C – Software Considerations in Airborne Systems and Equipment Certification
- DO-326A – Airworthiness Security Process Specification
- DO-355A – Information Security Guidance for Continuing Airworthiness
- DO-356A – Airworthiness Security Methods and Considerations
- DO-ISEM – Guidance on Information Security Event Management

Aeronautical Radio, Incorporated (ARINC)

- ARINC 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework
- ARINC Specification 823P1 DataLink Security, Part 1 - ACARS Message Security
- ARINC Specification 823P2 DataLink Security, Part 2 - Key Management
- ARINC Specification 834-8 Aircraft Data Interface Function (ADIF)
- ARINC Report 835-1 Guidance for Security of Loadble Software Parts Using Digital Signatures
- ARINC Project Paper 858: Internet Protocol Suite (IPS) for Aeronautical Safety Services - Technical Requirements
- ARINC Report 852 Guidance for Security Event Logging in an IP Environment
- ARINC Report 658 Internet Protocol Suite (IPS) for Aeronautical Safety Services - Roadmap Document
- ARINC Specification 664P1-2 Aircraft Data Network, Part 1, Systems Concepts and Overview

A4A (Airline for America, former ATA)

- ATA Spec 42 Aviation Industry Standards for Digital Information Security

European Standards (EN)

- BS EN 16495:2019 Air Traffic Management. Information security for organizations supporting civil aviation operations

Original Equipment Manufacturers (OEMs)

- Aircraft Security Guidance and Handbook, Maintenance Manual

4. Other Relevant Cyber Industry Framework

International Organization for Standardization (ISO)

- ISO/IEC/IEEE 15288:2015 Systems and software engineering—Systems life cycle processes
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management
- ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts
- ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements
- ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security

International Society of Automation

- ISA/IEC 62443-2-1:2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ISA/IEC 62443-3-3:2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels
- ISA/IEC-62443-4-2-2018 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

National Institute of Standards and Technology (NIST)

- NIST Framework for Improving Critical Infrastructure Cyber Security
- NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber Resilient Systems: A Systems Security Engineering Approach
- NIST SP 1900-202 Cyber-Physical Systems and Internet of Thing
- NIST IR 8259 Recommendations for IoT Device Manufacturers
- NIST IR 8259 Recommendations for IoT Device Manufacturers
- NIST IR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry

United Nations (UN)

- UN Security Council Resolution 2341
- The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices