



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

Edition 1.0, August 2020

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 continuously updated, considering the crucial developments and changes related to the regulations, standards, and guidance for aviation cyber security.

The list is divided into four following parts:

- International Instruments and Documents;
- European Regulations and Documents;
- National Documents and Guidance;
- Aviation Industry Cyber Specific Documents; and
- Other Relevant Cyber Industry Framework

Each part contains the name of the organization/owner of the document, brief description, status, tags, and the 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.

DISCLAIMER

The information contained in this document is subject to constant review in the light of changing government requirements and regulations. No subscriber or other reader should act on the basis of any such information without referring to applicable laws and regulations and/or without taking appropriate professional advice. Although every effort has been made to ensure accuracy, the International Air Transport Association shall not be held responsible for any loss or damage caused by errors, omissions, misprints, or misinterpretation of the contents hereof. Furthermore, the International Air Transport Association expressly disclaims any and all liability to any person or entity, whether a reader of this publication or not, in respect of anything done or omitted and the consequences of anything done or omitted, by any such person or entity in reliance on the contents of this document.

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 (URL Link)
International Air Law Instruments	Convention for the Suppression of Unlawful Seizure of Aircraft (1970)	<p>The Hague Convention of 1970 was adopted in order to combat aircraft hijacking. It contains provisions for the criminalization of offences that are committed on board an aircraft in flight when a person seizes or exercises control of the aircraft.</p> <p>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.</p>	In Force	#Legal_Instrument #Convention #Aircraft	https://treaties.un.org/pages/showDetails.aspx?objid=0800000280112834
	Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)	<p>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, as well as the acts, are likely to endanger the safety of aircraft in flight.</p> <p>As per the provisions of the Montreal Convention and its applicability, there is no requirement for the offender to be on board an aircraft in the time of committing the unlawful act. Therefore, this broadens the applicability scope of the Montreal Convention and could 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.</p>	In Force	#Legal_Instrument #Convention #Transversal	https://www.un.org/ruleoflaw/blog/document/convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-civil-aviation/
	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)	<p>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.</p> <p>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.</p>	In Force	#Legal_Instrument #Convention #Aerodromes	https://www.un.org/ruleoflaw/blog/document/protocol-on-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-civ/
	Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (2010)	<p>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 of that jurisdiction.</p> <p>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 the aircraft navigation. Moreover, the Beijing Convention addresses any attacks on such facilities and aircraft conducted by cyber means.</p>	In Force	#Legal_Instrument #Convention #Transversal	https://www.icao.int/secretariat/legal/Pages/TreatyCollection.aspx
	Beijing Supplementary Protocol to the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010)	<p>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.</p> <p>For the first time, the legal instrument directly refers to cyber security by including within its scope to 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.</p> <p>Therefore, the Beijing Supplementary Protocol of 2010 more directly covers cyber-attacks than any other international legal instrument within civil aviation.</p>	In Force	#Legal_Instrument #Convention #Aircraft	https://www.icao.int/secretariat/legal/Pages/TreatyCollection.aspx

International Civil Aviation Organization (ICAO)	Annex 17 – Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference	<p>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.</p> <p>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. Taking into consideration the definition of acts of unlawful interference, it needs to be noted that cyber-attacks may fall within its scope whenever they have an impact on aviation safety.</p> <p>Within the Annex 17, the 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</p>	In Force	#Legal_Instrument #SARPs #Transversal	https://www.icao.int/Security/SFP/Pages/Annex17.aspx
	Aviation Cybersecurity Strategy (2019)	<p>The ICAO Aviation Cybersecurity Strategy has endorsed during the 40th Session of the ICAO Assembly and published in 2019,</p> <p>Taking into consideration the multi-faceted and multidisciplinary nature of cyber security, as well as noting that cyber-attacks may rapidly affect a wide spectrum of areas, the works of ICAO aimed to deliver a common vision and define a set of global principles addressed by the Strategy.</p> <p>The Aviation Cybersecurity Strategy is aligned with other ICAO activities relative to cyber security, as well as coordinated with the safety and security management provisions.</p> <p>The goal of the Strategy will be achieved by the series of principles, measures, and actions addressed through the following seven pillars:</p> <ul style="list-style-type: none"> • International cooperation • Governance • Effective legislation and regulations • Cybersecurity policy • Information sharing • Incident management and emergency planning • Capacity building, training, and cybersecurity culture <p>Currently, the implementation action plan for the Strategy is under development process and should be published in the near future.</p>	In Force	#Legal_Instrument #Strategy #Transversal	https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
	Doc 8973 Aviation Security Manual (Restricted)	<p>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.</p> <p>This document is revised continuously in order to address new threats and technological improvements to prevent acts of unlawful interference.</p>	In Force	#SARPs #Guidance #Transversal	https://www.icao.int/Security/SFP/Pages/SecurityManual.aspx
	Doc 9985 Air Traffic Management Security Manual (Restricted)	<p>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.</p> <p>Moreover, this manual provides guidance relative to the ATSP on provisions of ATM security services in support of national security, as well as law enforcement requirements. It also provides guidance on the protection of the ATM system infrastructure against threats and vulnerabilities.</p>	In Force	#SARPs #Guidance #ATM/ANSP	https://www.icao.int/Pages/default.aspx
	Doc 10108 Global Risk Context Statement (Restricted)	<p>The Global Risk Context Statement (Doc 10108 – Restricted) contains a global aviation security risk assessment, including a global threat picture, as well as is intended to help inform and support States in the processes for national and local aviation security risk assessment.</p> <p>Appendix A of this document includes the risk assessment methodology and process map for the global risk assessment, as well as any other guidance to assist States with their national risk assessments.</p>	In Force	#Risk_Assessment #Guidance #Transversal	https://www.icao.int/Pages/default.aspx

	Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation	<p>The Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation supersedes the Assembly Resolution A39-19. This resolution introduced the ICAO Cybersecurity Strategy as well as instructed ICAO Secretary General to:</p> <ul style="list-style-type: none"> • 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	#Resolution #Transversal	https://www.icao.int/cybersecurity/Pages/Resources.aspx
--	---	--	-----------------	-----------------------------	---

European Regulations and Recommendations

This section is specifically related to the European regulations and recommendations, including also Strategy and/or guidance related to the aviation cyber security.

TABLE 2. EUROPEAN REGULATIONS AND RECOMMENDATIONS

Organization	Regulation / Standard / Recommendation Name	Purpose/Comments/Precis	Status	#Tag	Source (URL Link)
European Civil Aviation Conference (ECAC)	ECAC Doc 30, Part II (Restricted)	<p>The ECAC Doc 30, Part II Chapter 14, delivers recommendations relative to cyber security governance at the national level, as well as addresses activities at the organizational level. It represents a risk-based approach.</p> <p>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</p> <p>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.</p>	In Force	#Recommendation #Governance #Risk-Based_Approach #Transversal	https://www.ecac-ceac.org/web/guest
European Union (EU) Rulemaking	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	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> Contributing to the implementation of European Union rules in the area of cyber security; Ensuring the interdependencies between the different domains of aviation safety, and between aviation safety, cyber security and other technical domains of aviation regulation are considered and included in any activities. 	In Force	#Basic_Regulation #Common_Rules #Transversal	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139
	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	<p>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. This regulation is still in force; however, it will be amended by the Regulation (EU) 2019/1583.</p> <p>The Regulation provides detailed measures for the implementation of the common basic standards in order to safeguard civil aviation against acts of unlawful interference that jeopardize the security of civil aviation, as well as acts of unlawful interference posed by cyber threats.</p>	In Force	#Regulation #Security_Measures #Transversal	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1998
	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	<p>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.</p> <p>The amendment introduces detailed measures for the implementation of the common basic standards on aviation security as regards cyber security measures.</p>	Date of entry into force still unknown (pending notification) Date of effect: 31/12/2021	#Regulation #Security_Measures #Transversal	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.246.01.0015.01.ENG&toc=OJ%3AL%3A2019%3A246%3ATOC

	<p>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</p>	<p>The Regulation (EU) No 376/2014 on the reporting, analysis, and follow-up of occurrences in civil aviation 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 Industry.</p> <p>This regulation provides the means to increase information exchange between the Member States as well as ensures the continued availability of safety information.</p> <p>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.</p>	<p>In Force</p>	<p>#Regulation #Reporting #Safety_Information #Transversal</p>	<p>https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0376</p>
	<p>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</p>	<p>The Implementing Regulation (EU) 2017/373 introduced requirements for providers of Air Traffic Management/Air Navigation Services as well as other air traffic management network functions and their oversight.</p>	<p>In Force</p>	<p>#Regulation #Security_Measures #ATM/ANSP</p>	<p>https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0373&from=EN</p>
	<p>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)</p>	<p>The General Data Protection 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.</p>	<p>In Force</p>	<p>#Regulation #Data_Protection #GDPR #Transversal</p>	<p>https://eur-lex.europa.eu/eli/reg/2016/679/oj</p>
	<p>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</p>	<p>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 (NIS Directive).</p> <p>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:</p> <ul style="list-style-type: none"> • 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. 	<p>In Force</p>	<p>#Directive #Network_Security #Information_System #Security #Transversal</p>	<p>https://eur-lex.europa.eu/eli/dir/2016/1148/oj</p>
<p>European Aviation Safety Agency (EASA) Rulemaking</p>	<p>EASA RMT.0648 – Aircraft Cybersecurity</p>	<p>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).</p> <p>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.</p> <p>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.</p>	<p>Decision made on 24/06/2020, Entry into force to be determined.</p>	<p>#AMC #Network_Security #Information_System #Security #Aircraft</p>	<p>https://www.easa.europa.eu/document-library/rulemaking-subjects/aircraft-cybersecurity https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2020006r</p>

	EASA RMT.0720 – Management of Information Security Risks	<p>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).</p> <p>The main objective of these AMC is to efficiently contribute to the protection of the aviation system from cyber security attacks and their consequences. To achieve this objective, it is proposed to introduce provisions in all the aviation domains (design, production, continuing airworthiness management, maintenance, operations, aircrew, ATM/ANS, aerodromes).</p>	Ongoing, Decision scheduled for 2021/Q4.	#AMC #Risk_Management #Information_Security #Transversal	https://www.easa.europa.eu/document-library/rulemaking-subjects/cybersecurity-risks
European Strategic Coordination Platform (ESCP)	Strategy for Cyber Security in Aviation (2019)	<p>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.</p>	Published	#Strategy #Transversal	https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%202010%20September%202019.pdf

National Instruments and Documents

This section is specifically related to some national documents, strategies, and guidance on the aviation cyber security.

TABLE 3. NATIONAL DOCUMENTS AND GUIDANCE

Organization	Regulation / Standard / Recommendation Name	Purpose/Comments/Precis	Status	#Tag	Source (URL Link)
United Kingdom Civil Aviation Authority (CAA)	Aviation Cyber Security Strategy (2018)	The Aviation Cyber Security Strategy of 2018 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: <ul style="list-style-type: none"> • Understating the risk posed by cyber threats and existing vulnerabilities, and analyzing the consequences; • Managing cyber risks - take actions that are appropriate and proportionate; • Responding and recovering from cyber-attacks; and • Promoting cultural change, increasing capabilities, and raising awareness. 	Published	#Strategy #Transversal	https://www.gov.uk/government/publications/aviation-cyber-security-strategy
	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 the process of cyber security posture assessment within the aviation organization.	Published	#Cyber_Posture #Assessment #Transversal	https://publicapps.caa.co.uk/modalapplication.aspx?catid=1&pagetype=65&appid=11&mode=detail&id=9295
	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	#Oversight_Process #Transversal	https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=9242
Qatar Civil Aviation Authority (CAA)	Aviation Cyber Security Guidelines (2019)	The Aviation Cyber Security Guidelines , developed by the Qatar CAA, provides standards and principles relative to securing the critical aviation systems, as well as 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	#Guidance #Critical_Infrastructure #Transversal	https://www.caa.gov.qa/en-us/PrintedPublications/Pages/Aviation-Cyber-Security-Guidelines.aspx
United States Federal Aviation Administration (FAA)	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) introduces 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.	Published	#Advisory_Circular #Airworthiness #Aircraft	https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document/information/documentID/1028288

		NOTE: This Advisory Circular is not mandatory; it does not constitute a regulation. However, if used, you must conform to it in totality.		#Network_Security	
	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: <ul style="list-style-type: none"> • 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.	In Force	#Legal_Instrument #Transversal	https://fsims.faa.gov/PICResults.aspx?mode=EBookContents&restricttocategory=all~menu
	FAA Reauthorization Act of 2018, Public Law No: 115-254	The Reauthorization Act of 2018 sets provisions regarding the unmanned aircraft systems (UAS), cyber security, and any FAA activities in these terms.	In Force	#Legal_Instrument #Transversal	https://www.congress.gov/bill/115th-congress/house-bill/302/text?q=%7B%22search%22%3A%5B%22PL+115-254%22%5D%7D&r=1
	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). The goal of this regulation is to promote safe aviation, protect the crew, passengers, and the general public from unnecessary risk.	In Force	#Legal_Instrument #Transversal	https://www.law.cornell.edu/cfr/text/14
	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.	Published	#Policy #Aircraft #Certification #Transversal	https://www.icao.int/cybersecurity/SiteAssets/FAA/PS-AIR-21.16-02.pdf
	Cyber Security and Infrastructure Security Agency Act of 2018	The Cyber Security and Infrastructure Security Agency Act of 2018 amended the Homeland Security Act of 2002 and introduced the Cybersecurity and Infrastructure Security Agency (CISA), transferring the resources and responsibilities in terms of cyber security and infrastructure security to the agency.	In Force	#Legal_Instrument #Transversal	https://www.congress.gov/bill/115th-congress/house-bill/3359/text
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 that has been 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.	Published	#Advisory_Circular #Airworthiness #Aircraft #Network_Security	https://www.caas.gov.sg/docs/default-source/pdf/ac121-7-2(rev-0)-aircraft-network-security-programme-(ansp).pdf

Aviation Industry Cyber Specific Documents

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

TABLE 4. AVIATION INDUSTRY CYBER SPECIFIC DOCUMENTS

Organization	Regulation / Standard / Recommendation Name	Purpose/Comments/Precis	Status	#Tag	Source (URL Link)
International Air Transport Association (IATA)	Security Management System (SeMS) Manual, Edition 3 2019	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	#Guidance #Transversal	https://www.iata.org/en/publications/store/security-management-system-manual/
	Cyber Security Toolkit (2015)	The Cyber Security Toolkit provides guidance related to cyber threats and risks. The application is available as a web download or a floating license and offers: <ul style="list-style-type: none"> • Structured analysis tool to help identify, assess & mitigate risk; • Practical guidance material; • Complementary access to 17 training videos covering all aspects of IT Security; • Information reviewed by industry experts. 	Published	#Guidance #Transversal	https://www.iata.org/en/publications/store/aviation-cyber-security-toolkit/
Civil Air Navigation Services Organization (CANSO)	Cyber Security and Risk Assessment Guide	The Cyber Security and Risk Assessment Guide developed by CANSO provides an introduction to the cyber security relative to the ATM. The guidance includes the overview of the cyber threats and risks, some considerations for managing cyber risks, as well as some suggestions for implementing a cyber security program. Moreover, the guidance includes information on standards, a framework for cyber security as well as some practical guidance on the risk assessment.	Published	#Guidance #Risk_Assessment #ATM/ANSP	https://www.canso.org/canso-cyber-security-and-risk-assessment-guide#:~:text=The%20CANSO%20Cyber%20Security%20and,implementing%20a%20cyber%20security%20programme.
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	#Guidance #Aerodromes	https://store.aci.aero/product/cybersecurity-for-airport-executives-handbook/
	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	#Guidance #Aerodromes	https://store.aci.aero/product/pre-order-cybersecurity-implementation-handbook/
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. The purpose of this document is to help to ensure the safety of the flight and to maintain the operation of the aviation infrastructure without major disruptions. The scope of this guidance covers the design of aircraft, its production, and operations, ATM, aerodromes, maintenance, aviation service providers, components and information, as well as the supply chains. Currently, there are ongoing works on the update of ED-201, which will be replaced by the ED-201A.	Published Ongoing works on the ED-201A.	#Guidance #AISS #Transversal	https://www.eurocae.net/
	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. 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.	Published	#Guidance #Airworthiness #Design #Aircraft_Certification #OEM	https://www.eurocae.net/

		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.		#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.	Published	#Guidance #Airworthiness #Security #Aircraft	https://www.eurocae.net/
	ED-204 - Information Security Guidance for Continuing Airworthiness	The ED-204 - 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-204 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. Currently, ongoing works on the ED-204A.	Published	#Guidance #Continuous_Airworthiness #Security #Aircraft	https://www.eurocae.net/
	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 identify, evaluate, and manage impacts on safety, operational delivery as well as other commercial concerns. The ED-205 provides standards for certification or declaration of conformity with security requirements.	Published	#Standards #Guidance #Security_Certification #ATM/ANSP	https://www.eurocae.net/
	ED-XXX – Guidance on Security Event Management	The Information Security Event Management (ISMS) is currently in draft. Joint activity with RTCA DO-XYZ.	Ongoing (to be published in 2021)	#Guidance #Event_Management #Transversal	https://www.eurocae.net/
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	#Guidance #Maturity_Model #ATM/ANSP	https://www.eurocontrol.int/publication/atm-cybersecurity-maturity-model
	Monitoring Cyber Security Events – EATM-CERT Interactive Map	EUROCONTROL/EATM-CERT produced an interactive world map of publicly reported cyber events impacting aviation.	Published	#Cyber_Security_Event #Map #Transversal	https://www.google.com/maps/d/embed?mid=1ptVlma0CZqoPiN-zsomzbrVQDRS7BXGk&ll=20.231541030129446%2C0&z=2
RTCA	SC-216, Aeronautical Systems Security	The SC-216, Aeronautical Systems Security , delivers airworthiness security methods and considerations as a revision to DO-356. This is based on the Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security / Protection (ASISP) working group report. The aim of this document is to harmonize specific topics within DO-356 and EUROCAE ED-203. The guidance will help to ensure safe, secure, and efficient operations considering the integration of the electronic systems and network technologies onboard aircraft, for CNS/ATM systems, and aircraft operator operations and maintenance.	Published	#Guidance #Systems_Security #Airworthiness #Transversal	https://www.rtca.org/content/sc-216
	DO-178C, Software Considerations in Airborne Systems and Equipment Certification	The DO-178C, Software Considerations in Airborne Systems and Equipment Certification introduces recommendations for the production of software for airborne systems as well as	Published	#Guidance #Airborne_Systems	https://www.rtca.org/content/publications

		equipment that performs its intended function with a level of confidence in safety in compliance with the airworthiness requirements.		#Equipment_Certification	
	DO-326A, Airworthiness Security Process Specification	<p>The DO-326A, Airworthiness Security Process Specification provides additional guidance for aircraft certification for handling cyber threats to aircraft safety.</p> <p>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.</p> <p>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 changes to TC for installation and continued airworthiness for aircraft systems.</p>	Published	#Guidance #Airworthiness #Security #Aircraft	https://www.rtca.org/content/publications
	DO-355 - Information Security Guidance for Continuing Airworthiness	<p>The DO-355 - Information Security Guidance for Continuing Airworthiness provides guidance relative to the following stages of the product lifecycle: operation, support, maintenance, administration, and deconstruction.</p> <p>The DO-355 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.</p> <p>Currently ongoing work on the DO-355A.</p>	Published	#Guidance #Continuous_Airworthiness #Security #Aircraft	https://www.rtca.org/content/publications
	DO-356A - Airworthiness Security Methods and Considerations	<p>The DO-356A - Airworthiness Security Methods and Considerations provides guidance to protect the airworthiness of the aircraft from intentional unauthorized electronic interaction.</p> <p>This guidance provides methods and considerations to help prove compliance for airworthiness security during the entire lifecycle of aircraft.</p> <p>The DO-356A provides guidance to accomplish the airworthiness security process activities defined in the ED-202A / DO-326A.</p>	Published	#Guidance #Airworthiness #Design #Aircraft_Certification #OEM #Aircraft	https://www.rtca.org/content/publications
	DO-XYZ - Guidance on Security Event Management	The Information Security Event Management (ISMS) is currently in draft. Joint activity with RTCA EUROCAE ED-XXX.	Ongoing (to be published in 2021)	#Guidance #Event_Management #Transversal	https://www.rtca.org/
Aeronautical Radio, Incorporated (ARINC)	ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	<p>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.</p> <p>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 providing a common language in terms of understanding the security needs.</p>	Published	#Report #Framework #Information_Security #Aircraft	https://www.aviation-ia.com/products/811-commercial-aircraft-information-security-concepts-operation-and-process-framework-2
	ARINC Specification 823P1 DataLink Security, Part 1 - ACARS Message Security	<p>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.</p> <p>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.</p>	Published	#Standard #DataLink_Security #ACARS #Aircraft #Ground_Systems	https://www.aviation-ia.com/products/823p1-datalink-security-part-1-acars-message-security-2
	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.	Published	#Standard #DataLink_Security	https://www.aviation-ia.com/products/823p2-datalink-security-part-2-key-management-2

		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.		# Key_Management #Aircraft #Ground_Systems	
	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	#Standard #ADIF #Aircraft	https://www.aviation-ia.com/products/834-8-aircraft-data-interface-function-adif
	ARINC Report 835-1 Guidance for Security of Loadable 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	#Guidance #Loadble_Software #Digital_Signatures #Aircraft	https://www.aviation-ia.com/products/arinc-report-835-1-guidance-security-loadable-software-parts-using-digital-signatures-2
	ARINC Project Paper 858: Internet Protocol Suite (IPS) for Aeronautical Safety Services - Technical Requirements	The ARINC Project Paper 858 is a document with technical requirements and standards for airborne ATN/IPS systems. ATN/IPS aims to improve aviation safety communication services.	Ongoing	#Guidance #ATN/IPS	https://www.aviation-ia.com/activities/internet-protocol-suite-ips-aeronautical-safety-services
	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 and Entertainment Services (PIES). The ARINC Report 852 introduces a common set of security-related data elements and format(s) produced by aircraft systems.	Published	#Guidance #Loadble_Software #Digital_Signatures #Aircraft	https://www.aviation-ia.com/products/arinc-report-852-guidance-security-event-logging-ip-environment-2
	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	#Guidance #IPS #ATN/OSI #ATN/IPS #Aircraft	https://www.aviation-ia.com/products/658-internet-protocol-suite-ips-aeronautical-safety-services-roadmap-document
	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	#Standard #Data_Network #Aircraft	https://www.aviation-ia.com/products/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	The ATA Spec 42 Aviation Industry Standards for Digital Information Security delivers recommendations on standardized methods in order to achieve an appropriate level of security for the applications that rely on digital identities. This document aims to provide guidance to a different variety of stakeholders with security requirements.	Published	#Standard #Digital_Information #Transversal	https://publications.airlines.org/Commerce/ProductDetail.aspx?Product=294
European Standards (EN)	BS EN 16495:2019 Air Traffic Management. Information security for organizations supporting civil aviation operations	The BS EN 16495:2019 Air Traffic Management. Information security for organizations supporting civil aviation operations provides guidance that is based on the EN ISO/IEC 27002:2017 applicable to the organizations that support civil aviation, focusing on the ATM operations.	Published	#Standard #Information_Security #ATM/ANSP #Transversal	https://www.en-standard.eu/bs-en-16495-2019-air-traffic-management-information-security-for-organisations-supporting-civil-aviation-operations/
Original Equipment Manufacturers (OEMs)	Aircraft Security Guidance and Handbook, Maintenance Manual	Each OEM provides guidance material upon delivery with methods and specifications for the security of the aircraft and its network.	/	#Aircraft #Security	/

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 5. OTHER RELEVANT CYBER INDUSTRY FRAMEWORK

Organization	Regulation / Standard / Recommendation Name	Purpose/Comments/Precis	Status	#Tag	Source (URL Link)
International Organization for Standardization (ISO)	ISO/IEC/IEEE 15288:2015 Systems and software engineering—Systems life cycle processes	<p>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.</p> <p>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.</p>	Published	#Standard #System_Engineering #Software_Engineering #Life_Cycle #Transversal	https://www.iso.org/standard/63711.html
	ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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	#Standard #Information_Technology #Security_Techniques #Security_Management #Transversal	https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls	<p>The ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls provides guidance on the information security standards and information security management practices within the organization. This includes the selection, implementation, and management of controls.</p> <p>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.</p>	Published	#Standard #Information_Technology #Security_Techniques #Security_Controls #Transversal	https://www.iso.org/standard/54533.html
	ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management	<p>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 based that is based on a risk management approach.</p> <p>The standards of ISO/IEC 27005:2018 can be applied by different types of organizations with an intent to manage risks that can compromise the information security of the organization.</p>	Published	#Standard #Information_Technology #Security_Techniques #Risk_Management #Transversal	https://www.iso.org/standard/75281.html
	ISO/IEC 27036:2013+ — Information technology — Security techniques — Information security for supplier relationships	<p>The ISO/IEC 27036:2013+ — Information technology — Security techniques — Information security for supplier relationships delivers standards and guidance on the evaluation and treatment of information risks in terms of relations with suppliers.</p>	Published	#Standard #Information_Technology #Security_Techniques #Supplier_Relationships #Transversal	https://www.iso27001security.com/html/27036.html

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 in terms of the cyber security management system to be used in the industrial automation and control systems environment.	Published	#Standard #Security_Program #Industrial_Automation #Control_Systems #Transversal	https://www.isa.org/
	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	#Standard #Industrial_Automation #Security_Requirements #Security_Levels #Transversal	https://www.isa.org/
	ISA/IEC-62443-4-2 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	#Standard #Industrial_Automation #Security_Requirements #IACS_Components #Transversal	https://www.isa.org/
National Institute of Standards and Technology (NIST)	NIST Framework for Improving Critical Infrastructure Cyber Security	The NIST Framework for Improving Critical Infrastructure Cyber Security introduces information on the voluntary risk management framework that includes: <ul style="list-style-type: none"> standards; guidelines; and best practices to manage cybersecurity-related risk. <p>The NIST framework is a prioritized, flexible, and cost-effective approach to help to promote the protection and resilience of critical infrastructure.</p>	Published	#Standard #Framework #Critical_Infrastructure #Transversal	https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-1.1
	NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy	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, representing a disciplined, structured, as well as a flexible process for managing security and privacy risk.	Published	#Standard #RMF #Information_Systems #Life_Cycle #Security&Privacy #Transversal	https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
	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	#Standard #Information_Security #Risk_Management #Transversal	https://csrc.nist.gov/publications/detail/sp/800-39/final
	NIST SP 800-53 Rev 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations	The NIST SP 800-53 Rev 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations delivers a set of security and privacy controls applicable to federal information systems and organizations as well as a process on how to select controls in order to protect the operations, assets, individuals of the organization, other organizations, as well as the Nation from a diverse set of cyber threats.	Published	#Standard #Security_Controls #Privacy_Controls #Transversal	https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news
	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	Published	#Standard #ICS	https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

		Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), as well as other control system configurations.		#Transversal	
	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 the guidance from the engineering-driven perspective as well as actions that are necessary for the development of more secure and survivable systems.	Published	#Standard #Security_Engineering #Transversal	https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
	NIST SP 800-160 Vol. 2 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	#Standard #Security_Engineering #Cyber_Resiliency #Transversal	https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final
	NIST SP 1900-202 Cyber-Physical Systems and Internet of Things	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	#Standard #CPS #IoT #Transversal	https://www.nist.gov/publications/cyber-physical-systems-and-internet-things
	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	#Recommendation #IoT #Device_Manufacturers	https://csrc.nist.gov/publications/detail/nist-ir/8259/final
United Nations (UN)	UN Security Council Resolution 2341, 2017	The UN Security Council Resolution 2341 recognizes and addresses the growing importance of ensuring the reliability and resilience of critical infrastructure, as well as its protection from terrorist attacks for national security.	Published	#Resolution #Security #Critical_Infrastructure #Transversal	http://unscr.com/en/resolutions/doc/2341
	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 coming 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 for the protection of critical infrastructure from terrorist attacks, including cyber aspects.	Published	#Guidance #Critical_Infrastructure #Transversal	https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

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
- Aviation Cyber Security Strategy (2019)
- 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

2. European Regulations and Documents

European Civil Aviation Conference (ECAC)

- ECAC Doc 30, Part II (Restricted)

European Union (EU) Regulations

- 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
- 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
- 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
- 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
- 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 Aviation Safety Agency (EASA) Rulemaking

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

European Strategic Coordination Platform (ESCP)

- Strategy for Cyber Security in Aviation (2019)

3. National Documents and Guidance

United Kingdom (Civil Aviation Authority)

- Aviation Cyber Security Strategy (2018)
- CAP1850: Cyber Assessment Framework (CAF) for Aviation
- CAP1753: CAA Cyber Security Oversight Process for Aviation

Qatar (Civil Aviation Authority)

- Aviation Cyber Security Guidelines (2019)

United States (Federal Aviation Administration)

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

Singapore (Civil Aviation Authority of Singapore)

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

4. Aviation Industry Cyber Specific Documents

International Air Transport Association (IATA)

- Security Management System (SeMS) Manual, Edition 3 2019
- Cyber Security Toolkit (2015)

Civil Air Navigation Services Organization (CANSO)

- Cyber Security and Risk Assessment Guide

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-204 - Information Security Guidance for Continuing Airworthiness
- ED-205 - Process Standard for Security Certification and Declaration of ATM ANS Ground Systems
- ED-XXX – Guidance on Security Event Management

EUROCONTROL

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

RTCA

- SC-216, Aeronautical Systems Security
- DO-178C, Software Considerations in Airborne Systems and Equipment Certification
- DO-326A, Airworthiness Security Process Specification
- DO-355 - Information Security Guidance for Continuing Airworthiness
- DO-356A - Airworthiness Security Methods and Considerations
- DO-XYZ - Guidance on 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 Loadable 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

5. 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 27036:2013+ — Information technology — Security techniques — Information security for supplier relationships

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 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. 4 Assessing Security and Privacy Controls in Federal 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 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

United Nations (UN)

- UN Security Council Resolution 2341, 2017
- The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices