International Civil Aviation Organization

The Eighth Meeting of the APANPIRG ATM Sub-Group

Bangkok, Thailand, 23 – 27 November 2020

Agenda Item 9: Any other business

AIR TRAFFIC MANAGEMENT SECURITY AND CYBERSECURITY

(Presented by the Secretariat)

SUMMARY

This paper presents information on Air Navigation Service Providers (ANSP) and Air Traffic Management ICAO security requirements and additional information relating to the establishment and dissemination of the 1st Edition of the ICAO Cyber Security Action Plan and ongoing developments in related guidance material and resources.

1. INTRODUCTION

1.1 Aviation security SARPs are contained in Annex 17 - *Security* and have relevance to many other Annexes including, but not limited to, Annex 2, 6, 8, 9, 10, 11, 14 and 18. There are also connections with PANS Docs 4444 and 8168.

1.2 Annex 17 – *Security* requires States to develop and implement a National Civil Aviation Security Programme (NCASP), which should specify the roles and responsibilities of all the organizations and agencies, including Air Traffic Services (ATS) Providers, that may be involved in security operations. The NCASP addresses the whole range of security activities including, *inter alia*, threat and risk assessment, staff selection and training (in security-related matters), access control and other preventive security measures, management of response to acts of unlawful interference, and quality control.

1.3 Not all provisions of the NCASP will be applicable to the ANS Providers. The NCASP identifies the specific responsibilities of each of the parties that have a role in security operations.

2. DISCUSSION

2.1 There are a number of Standards and Recommended Practices (SARPs) with particular relevance to ATS Providers and ATM security contained in the latest Amendment 16 of Annex 17 – *Security* applicable as of 16 November 2018. Amendment 16 contains several new provisions that have a bearing on Air Traffic Management Security Requirements in addition to those established in the previous Amendment 15 to the Annex including primarily Standard 3.5 but also to varying degrees, a number of additional SARPs with direct relevance as noted in previous papers to this meeting.

2.2 States' compliance with the above mentioned SARPs are subject to auditing under the ICAO Universal Security Audit Programme - Continuous Monitoring Approach (USAP-CMA).

2.3 In accordance with its leadership role, and in recognition of the vital role played by ATSPs and the security of ATM, ICAO has drafted guidance to assist States to establish and implement the appropriate security provisions as required by the relevant SARPs which would include the physical and electronic protection of all relevant facilities and equipment. The Air Traffic Management Security Manual (Doc 9985) is available to States for convenience. This Manual complements the *Aviation Security Manual* (Doc 8973 – Restricted) and provides guidance on security issues specific to ATM in order to assist States and ATS Providers in implementing appropriate security provisions to meet the published requirements of the NCASP. In addition, the manual provides guidance to the ATS Providers on provision of ATM security services in support of national security and law enforcement requirements, and guidance on protection of the ATM system infrastructure from threats and vulnerabilities.

2.4 The 11th Edition of the ICAO Aviation Security Manual (Doc 8973) incorporates guidance material relating to cyber security. The 2nd Edition of the ICAO global Risk Context Statement (RCS) ICAO Doc 10108 (2019) provides a methodological approach to Risk assessment (including ATM/cyber risks) – to support States in developing their national threat/risk evaluation/mitigation system. The 2nd Edition Doc 10108 of the global RCS continues to define the risk of cyber security attacks used as an act of unlawful interference against civil aviation as low. This is further established in the 2020 document entitled "Updated Overview of Threats and Risks to Civil Aviation" (EB 2020/45 dated 25 September 2020 refers). However, this is in a global risk context and assessed in regard to all potential forms of acts of unlawful interference with civil aviation. The risk level may vary based on individual States own risk assessments and/or risk assessments conducted by relevant agencies for their own environment and operations.

Cybersecurity Initiatives and Projects

Progress report of the Secretariat Study Group on Cybersecurity (SSGC)

2.5 To date, the SSGC conducted eight meetings the last of which was held in 5 October 2020 virtually via online platform. The Eighth Meeting of the SSGC, originally scheduled to take place in May 2020, was postponed due to resource constraints and the COVID-19 pandemic.

2.6 The impact of the pandemic on civil aviation highlighted the need for States and stakeholders to address cyber threats, considering the widespread use of virtual means for conducting meetings due to the restrictions on travel, the parking of aircraft for a long period of time and the potential impact on the security of its systems, as well as the impact on the aviation workforce in terms of availability and currency of personnel to adequately perform their duties.

2.7 The above developments contributed to the need for the SSGC to continue its work in a virtual manner, albeit at a reduced pace due to the impact of the pandemic and the shift in priorities of States and stakeholders towards the restart and recovery of air transport operations.

2.8 The eight meeting of the SSGC which convened virtually on 5 October 2020 addressd the following issues:

Finalize the Cybersecurity Action Plan to be communicated to States and stakeholders for implementation;

Address Cybersecurity in the context of COVID-19 and the restart of air transport;

Receive a brief on the work of the Trust Framework Study Group (TFSG);

Review the work of the SSGC Sub-Groups; and

Define the future work programme of the SSGC.

Cybersecurity Action Plan (CyAP)

2.9 The 1st Edition of the ICAO Cybersecurity Action Plan (CyAP) has been disseminated by ICAO State Letter ICAO State Letter AS8/1.9.1-20/114 - dated 5 November 2020. The CyAP itself is attached to the letter as the Enclosure. The CyAP is a document that aims at supporting States and stakeholders in implementing the Cybersecurity Strategy, through proposing a series of principles, measures, and actions to achieve the objectives of the Cybersecurity Strategy's seven pillars. It provides the foundation for ICAO, States and stakeholders to work together to develop the ability to identify, prevent, detect, respond to, and recover from cyber-attacks on civil aviation as well as create a solid framework for cooperation between all concerned stakeholders.

2.10 Following the comments received from the 219th Session of the Council on the initial draft then presented, the SSGC reviewed the document, addressed the comments received from the Council, and finalized the 1st Edition of the Cybersecurity Action Plan.

3.7 The CyAP is a living document which will be updated as required in-line with the changes in the cybersecurity threat landscape as well as the technological and other developments affecting cybersecurity in aviation.

Cybersecurity Training Roadmap

2.11 In order to support the Cybersecurity Strategy and the Cybersecurity Action Plan, the Secretariat has developed during 2020 a Cybersecurity Training Roadmap so that ICAO can build the capability to deliver appropriate, coherent and relevant Aviation Cybersecurity training to States and stakeholders. This will include the provision of materials and expertise to support regional activities and events to further assist States in addressing this topic.

2.12 The development of the ICAO Cybersecurity Training Roadmap also supports Assembly Resolution A40-25: *Implementing Aviation Training and Capacity Building Strategies*, which lays out how ICAO, through training activities, shall assist and support States with the development of sufficient human resources and capacity. With a global shortage of trained cybersecurity personnel across multiple sectors, a synchronized and strategic effort, such as this one, is essential to ensure that States have personnel who are able to support national aviation cybersecurity demands.

Progress report of Trust Framework Study Group (TFSG)

2.13 The Trust Framework Study Group has been advancing its work on a concept of operations (ConOps) to reduce the cyber-attack surface in a digitally connected environment through processes and procedures for digital identity management, use of logically isolated networks and use of dedicated block of digital addresses for different systems and members of the aviation community. The work is focused on assurance of cyber secure and resilient communication between ground-ground, air-ground and air-air systems to meet the requirements of confidentiality, integrity and availability of digital communication systems.

2.14 The TFSG also continues, in coordination with different Air Navigation Commission Panels, its work to produce harmonized procedures and guidance material aligned with existing industry work and with future requirements of new entrants for operations in a non-segregated airspace.

Feasibility Study on the Mechanism to Address the ICAO Cybersecurity Work Programme

2.15 The progress of work on the feasibility study was hindered by some resource constraints faced by the Secretariat in the first half of 2020. In February 2020, the Secretariat lost most of its cybersecurity resources – namely its Cybersecurity Officer and the Cybersecurity Consultant assisting with the study – both working in the Air Transport Bureau. The recruitment and renewal of positions, including the Cybersecurity Officer and the Consultant, had been frozen as a result of the financial situation of the Organization in the first half of 2020 as one measure to address the financial situation due to delays in State assessment payments, as reported to the Council. The recruitment process for the replacement of the technical officer had been initiated in fall 2019, but the new Cybersecurity Officer only reported for duty at the beginning of August 2020, while the Consultant resumed work in September.

2.16 As such, the Secretariat is recommencing its work on the feasibility study with high priority, including the required coordination within ICAO with the aim to report the outcome to Council for consideration during its 222nd Session.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) make use of the relevant available guidance material and resources;

c) ensure regulatory compliance with the International and National requirements for ATS Providers and ATM Security;

d) encourage States that already have security provisions in place for air traffic service providers to share information with other States;

e) continue to support the outcomes of the 40th Session of the ICAO Assembly in September 2019 as they relate to the new ICAO Cybersecurity Strategy;

f) Monitor the output of and participate as applicable, the ICAO Cyber Security Study Group, Cybersecurity Plan, Training Roadmap and development of Trust Framework;

g) In accordance with the ICAO State Letter AS8/1.9.1-20/114 - dated 5 November 2020. disseminate the Cybersecurity Action Plan and coordinate its implementation with all relevant national agencies, industry, and stakeholders; and

h) develop and establish national cyber security plans and priorities to provide a framework for action.

— END —

International Civil Aviation Organization | Organisation de l'aviation civile internationale | Organización de Aviación Civil Internacional | Международная организация гражданской авиации | منظمة الطيران المدني الدولي | 国际民用航空组织

Tel.: +1 514-954-8219 ext. 6760

Ref.: AS8/1.9.1-20/114

5 November 2020

Subject: Cybersecurity Action Plan

Action required: a) disseminate the Cybersecurity Action Plan and coordinate its implementation with all relevant national agencies, industry, and stakeholders; and b) develop and establish national plans and priorities to provide a framework for action

Sir/Madam,

1. I have the honour to refer to the International Civil Aviation Organization (ICAO) Assembly Resolution A40-10, *Addressing cybersecurity in civil aviation*, which, inter alia, requested the development of a Cybersecurity Action Plan to support implementation of the Cybersecurity Strategy by States, industry, and stakeholders.

2. The Cybersecurity Action Plan was approved by the ICAO Council during its Second Meeting of the 219th Session on 4 March 2020. Prior to its dissemination to Member States, and recognizing that the Cybersecurity Action Plan is a living document, the Secretariat made further updates in order to take into account the comments and inputs of various ICAO's governing bodies and technical expert groups, received until 5 October 2020.

3. Accordingly, I am pleased to provide you with the attached First Edition of the Cybersecurity Action Plan. The Plan comprises principles, measures, and proposed actions to achieve the objectives of the Cybersecurity Strategy's seven pillars. It provides a framework for cooperation between all concerned stakeholders to develop the ability to identify, prevent, detect, respond to, and recover from cyber-attacks on civil aviation. As a living document, the Plan will be updated as and when required.

4. It is important that national plans and priorities be developed and implemented, ensuring they are aligned with the Plan, where applicable. I would also be grateful that ICAO be regularly informed on these efforts, the Plan's implementation status, as well as any challenges faced thereupon.

Accept, Sir/Madam, the assurances of my highest consideration.

Fang Liu
Secretary General

Enclosure:
Cybersecurity Action Plan

999 Robert-Bourassa Boulevard
Montréal, Quebec
Canada H3C 5H7

Tel.: +1 514-954-8219
Fax: +1 514-954-6077

Email: icaohq@icao.int
www.icao.int

Cybersecurity Action Plan

Published by authority of the Secretary General

November 2020

International Civil Aviation Organization

Terms and definitions[1]

caISMS : civil aviation Information Security Management System

A model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve civil aviation objectives based upon a risk assessment and the organization's risk acceptance levels designed to treat and manage risks. Source ISO27000:2009.

Cybersecurity

The term 'Cybersecurity' is used in this document alternatively with the term 'Information Security.'

Cybersecurity Policy

A cybersecurity policy documents the intentions and direction of an organization, for the management of cybersecurity threats, as expressed by top management. It is a written document in an organization outlining how to protect the organization from cybersecurity threats, and how to handle situations when they do occur. The cybersecurity policy must identify all of an organization's assets as well as all the potential threats to those assets. Employees need to be kept updated on the organization's security policies. The policy itself should be updated regularly as well.

Event (Information security)

Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failures of control, or a previously unknown situation that may be security relevant [ISO/IEC 27035]. It shall be noted that 'occurrence' needs to be considered in its broad sense and shall not be understood as (safety) occurrence term that only embraces the events which have, or could have significance in the context of aviation safety.

Incident (Information security)

Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC 27035-1]

Information Security

Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved. [BS ISO/IEC 27000:2018]

Information Sharing

The exchange of a variety of network and information security-related information such as risks, vulnerabilities, threats and internal security issues as well as good practice.

RCS: Risk Context Statement

Annual report on global risks written by the ICAO Threat and Risk Working Group based on its analysis.

Risk matrix

Tool for ranking and displaying components of risks (threat, consequence and vulnerability) and ultimately the residual risks.

[1] Still under review by the SSGC/RSGLEG

Threat source (or actor)

Entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact –- an organization's security, e.g.: terrorist, criminal, hacker, hacktivist, etc.

Vulnerability

Features of something potentially under threat which can be exploited by an attacker e.g. at an airport or on an aircraft, or which mean the asset may be inadvertently affected by a deliberate act of interference against a non-aviation target, combined with any weakness in current security measures.

EXECUTIVE SUMMARY

The 39th Session of the International Civil Aviation Organization (ICAO) Assembly reaffirmed the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber-attacks, and obtaining global commitment for action by ICAO, its Member States and industry stakeholders, with a view to collaboratively and systemically addressing cybersecurity in civil aviation and mitigating the associated threats and risks. Resolution A39-19 – *Addressing Cybersecurity in Civil Aviation* identified the actions to be undertaken by States and other stakeholders in this regard. The 39th Session of the ICAO Assembly also instructed ICAO to develop a comprehensive cybersecurity work plan.

In order to meet the expectations of the Assembly, a Cybersecurity Strategy for civil aviation was developed by the Secretariat Study Group on Cybersecurity (SSGC).

The 40th Session of the ICAO Assembly adopted the amended Resolution A40-10 – *Addressing Cybersecurity in Civil Aviation*, which calls upon States to implement the Cybersecurity Strategy and underlines the importance of developing a sustainable implementation plan for the Strategy, as well as continuing the work for the development of a strong cybersecurity framework.

The Cybersecurity Action Plan (CyAP) provides the foundation for States, industry, stakeholders and ICAO to work together to develop the ability to identify, prevent, detect, respond to and recover from cyber-attacks on civil aviation as well as create a solid framework for cooperation. It has been developed with the aim to propose a series of principles, measures and actions to achieve the objectives of the strategy's seven pillars.

Priority Outcome	**1. DEVELOP A GLOBAL AND AGREED VISION**	**WHO**	**WHEN**
Priority Actions	• Recognize that it is imperative to develop a comprehensive and agreed cybersecurity vision as a foundation to solid and coordinated global aviation cybersecurity risk management; • Recognize that the civil aviation sector shall be resilient to cyber-attacks and remain safe and trusted globally, whilst continuing to innovate and grow; • Recognize that cybersecurity risks fall under the convention on International Civil Aviation.	ICAO, Member States, and Industry	2020

Priority Outcome	**2. ACHIEVE INTERNATIONAL COOPERATION**	**WHO**	**WHEN**
Priority Actions	• Develop cooperation at national and international levels; • Mutual recognition of the efforts (develop, maintain and improve cybersecurity) to protect civil aviation; • Achieve harmonization at global, regional and national levels in order to promote global coherence and ensure interoperability of protection measures; • Engage States in addressing cybersecurity in international civil aviation; • Facilitate and promote international events in the cybersecurity field.	ICAO, Member States, and Industry	On-going

Priority Outcome	3. DEVELOP GOVERNANCE AND ACCOUNTABILITY	WHO	WHEN
Priority Actions	• Encourage, support and build upon the ICAO Cybersecurity Strategy; • Develop clear national governance and accountability for civil aviation cybersecurity; • Ensure coordination at State level between civil aviation authorities and competent national authorities for cybersecurity; • Establish appropriate coordination channels among various State authorities and industry; • Include cybersecurity in national civil aviation safety and security programmes; • Include cybersecurity in global and regional plans; • Work towards a common baseline for cybersecurity Standards and Recommended Practices.	ICAO, Member States, and Industry	2020

Priority Outcome	4. DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS	WHO	WHEN
Priority Actions	• Ensure that international legal instruments provide appropriate measures for the prevention, prosecution and timely reaction to cyber incidents. • Ensure that appropriate regulations and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and industry in implementing cybersecurity-related provisions;	ICAO, Member States, and Industry	2022-2023

Priority Outcome	5. DEVELOP A CYBERSECURITY POLICY	WHO	WHEN
Priority Actions	• Ensure that cybersecurity is part of the aviation security and safety systems and the comprehensive risk management framework; • Ensure varying risk assessment methodologies to retain comparability; • Develop cybersecurity policies considering the complete life cycle of aviation systems.	ICAO, Member States, and Industry	2022-2023

Priority Outcome	6. DEVELOP INFORMATION-SHARING CAPABILITIES	WHO	WHEN
Priority Actions	• Develop information sharing platforms and mechanisms, in line with existing ICAO provisions, to allow prevention, early detection and mitigation of relevant cybersecurity events.	ICAO, Member States, and Industry	2022-2023

Priority Outcome	**7. DEVELOP INCIDENT MANAGEMENT AND EMERGENCY PLANNING**		
Priority Actions	• Ensure appropriate and scalable plans that provide for continuity of air transport during cyber incidents; • Encourage the use of existing contingency plans and include provisions for cybersecurity and conduct exercises to test cyber resilience.	ICAO, Member States, and Industry	2022-2023
Priority Outcome	**8. DEVELOP CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE**	**WHO**	**WHEN**
Priority Actions	• Ensure qualification of personnel in both aviation and cybersecurity; • Increase awareness about cybersecurity; • Ensure proper curricula on aviation cybersecurity are included in the national educational framework at the professional development level, in order to ensure the development of a cross aviation safety and security body of knowledge throughout the organization including its senior management; • Foster cybersecurity innovation and appropriate research and design; • Include cybersecurity in the ICAO Next Generation of Aviation Professionals' strategy.	ICAO, Member States, and Industry	2022-2023

Chapter 1

INTRODUCTION

1.1. BACKGROUND

1.1.1. In the current civil aviation context, air traffic is always projected to increase over the long term, technology evolves swiftly, airspace users and operations are becoming more complex, and the operational environment consequently becomes more challenging. Rapid technological changes are altering the way civil aviation operates and making the system more vulnerable to cybersecurity threats. Malicious cyber activity can affect civil aviation in a variety of ways, from a small disruption of operations to catastrophic events. Risks are growing rapidly and there is a strong need for a sustainable cybersecurity framework at the international, regional and national levels.

1.1.2. Building a robust cybersecurity infrastructure, which relies on strong cooperation among States, industry, and ICAO, enables the creation of a common cybersecurity awareness that will ultimately lead to a more secure and resilient civil aviation system.

1.1.3. ICAO is constantly adapting to meet the ever-evolving global threat picture, in line with thr United Nations Security Council's resolutions that affirm States' responsibility to ensure the safety of air services operating within their territory and call upon all States to work with ICAO to ensure that international security standards are reviewed, updated, and put in place, based on current risks, pursuant to the Chicago Convention. As cybersecurity threats to civil aviation are evolving and will likely increase in prevalence, following the provisions of UNSCR 2341 (2017), ICAO is focused on establishing appropriate mechanisms to mitigate and reduce risks to aviation critical infrastructure from unlawful interference through cyber vectors and from any event that may jeopardize the resilience of systems that may impact safety of operations.

1.1.4. In this respect, in order to properly achieve the objectives of the seven pillars of the Aviation Cybersecurity Strategy and to shape a cybersecurity framework, this Action Plan has been developed.

1.2. PURPOSE

1.2.1. This Plan is a living document that will evolve with developments in cybersecurity and will be regularly updated to reflect the required changes stemming from, among other things, the gap analysis and activities described in Chapters 3 and 4. The CyAP captures the objectives and actions to be achieved for the implementation of the ICAO Aviation Cybersecurity Strategy. The elements presented in this document reflect the work done or that is currently ongoing within different regions/States or industry. It encompasses the results of analysis of the current "as-is" situation of the aviation system from a cybersecurity perspective, when compared to the "to-be" situation proposed in the strategy, elaborating on an action plan that can drive such evolution towards the strategic vision.

1.2.2. Given the significant work required in implementing the objectives and actions set out in this document, a staged approach, identifying short, medium and long-term targets, is proposed in Appendix A.

1.3. RISK CONTEXT

1.3.1. Cybersecurity is not a new concept to civil aviation. However, as cybersecurity threats have become increasingly prevalent, it has become one of the centrepieces when discussing and analysing risks to and vulnerabilities of the civil aviation system. The civil aviation sector is particularly at risk, because cyber-attacks are more likely to be successful in a sector which components are growing in a functionally and digitally interdependent way, and also because the cyber-defence mechanisms currently in use by the civil aviation sector are not yet adequate to deal with this persistent and adaptive threat.

1.3.2. The ICAO *Aviation Security Global Risk Context Statement* (Doc 10108) most recently evaluated the level of risk stemming from the exploitation by cyber-attackers, with a terrorist profile, as low. This assessment is based on residual vulnerability in the cybersecurity field, assuming that States have effectively implemented Annex 17 – *Security* provisions. However, cyber risks are rapidly evolving and they must be assessed for all cyber-attacker profiles that could affect not only security but also safety of civil aviation operations. Furthermore, the source of cyber-attacks is often difficult to trace, and, as such, the responsible persons cannot be prosecuted, as attribution and prosecution of cyber-attacks is often complicated and difficult to accomplish, while leaving the victim of the attack to bear the recovery costs. For these reasons, it is of extreme importance that ICAO, States and industry join forces and implement the Cybersecurity Strategy in a systematic manner.

1.4. BENEFITS OF THE ACTION PLAN

1.4.1. The CyAP aims at ensuring the commitment of ICAO, Member States, and industry to undertake their responsibilities in the implementation of the Cybersecurity Strategy and achieve the objectives outlined in its seven pillars. A strong cybersecurity framework will strengthen the civil aviation system and will be beneficial to the entire global aviation community.

Chapter 2

OBJECTIVE

2.1. OBJECTIVE OF THE CYBERSECURITY ACTION PLAN

2.1.1. The goal of the Cybersecurity Action Plan is to achieve the objectives outlined in each of the seven pillars of the Cybersecurity Strategy, as well as the development of a robust civil aviation cybersecurity framework.

2.1.2. The principles that form the foundation of the present Action Plan are:

a) understanding by Member States of the obligations they have with respect to cybersecurity deriving from the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation operations;

b) coordination of aviation cybersecurity measures amongst State authorities to ensure effective and efficient global management of cybersecurity; and

c) commitment of all civil aviation stakeholders to further develop cyber-resilience and protect aviation against cyber-attacks, originating from whatever threat source profile, that might impact safety, security and continuity of the air transport system.

2.2. APPLICATION

2.2.1. This document is primarily targeted at ICAO Member States and industry, as a means to manage cybersecurity risks in civil aviation, through a comprehensive, coordinated and holistic approach.

2.2.2. States, industry and other relevant stakeholders should undertake the actions stemming from this action plan.

Chapter 3

FOUNDATIONS OF THE CYBERSECURITY ACTION PLAN

3.1 KEY PRIORITIES

3.1.1 ICAO's vision for global civil aviation cybersecurity is for the aviation sector to be resistant and resilient to cyber-attacks and to remain safe, secure and trusted globally, whilst continuing to adapt, innovate and grow. The cybersecurity work programme aims at supporting this objective to ensure the current and future aviation system is a trustworthy and dependable environment, so that aviation stakeholders will be able to rely on products, services and information provided by others for the accomplishment of their operational objectives.

3.1.2 This action plan is intended to focus resources and actions to achieve a systemic approach to cybersecurity management in civil aviation, including current and legacy systems, with the ultimate objective to develop a system-of-systems approach that enables civil aviation to adapt in a timely fashion, and, therefore, to withstand new threats without significant disruptions. Given the urgency to protect civil aviation from cyber-attacks, ICAO must take stock of and build on existing, in-progress civil aviation cybersecurity initiatives and call for, as a baseline measure, the implementation of the basic baseline security measures typically implemented in any information technology/operational technology (IT/OT) system (e.g. appropriate cyber hygiene) including the implementation of the existing cyber security Standards and Recommended Practices in Annex 17. The guiding policy for the course of action should then be to channel ICAO actions. These objectives can be met by focusing attention on four main directions:

a) Establish a cybersecurity culture. The aviation industry has made considerable progress in the past decades through the deployment of innovative technologies and by harnessing increasing amounts of data. However, over this time, new threats have emerged. The aspirational goal is to establish a cybersecurity culture in aviation that aligns with the existing notions of safety and security cultures and ingrains cybersecurity in the lifecycle of a system.[2]

b) Ensure civil aviation is a cyber-resilient system. A cyber-resilient civil aviation system is a system that, under attack, can maintain its critical functionalities: i.e., supports safe and secure flight operations with minimal, if any, disruption. It mitigates the adverse effects of cyber-attacks as quickly as possible and to the maximum extent possible, through a holistic multi-layered protection approach. This approach should ensure that a successful attack on one layer, (e.g., an authentication breach that allows intrusion), does not compromise other layers of the system and/or lead to loss of safety or continuity of critical functions. The system should also adopt a continuous improvement approach to ensure that necessary adaptations to planned technical or procedural evolutions are made and kept up-to-date and that changes and continuous improvements are applied to incorporate lessons learned. Finally, the system should include appropriate cooperation and information-sharing mechanisms between

[2] The ICAO Safety Management Manual (Doc 9859) defines System as an organized, purposeful structure that consists of interrelated and interdependent elements and components, and related policies, procedures and practices created to carry out a specific activity or solve a problem.

aviation stakeholders, such as government, industry and, where appropriate, between civil and military authorities.

c) Ensure civil aviation is self-strengthening by adopting a "built-in security" approach. Adopting a built-in security approach for civil aviation requires, at the outset of a system's conception, consideration of security objectives that need to be achieved during a system's design process, along with traditional operational and safety objectives. Ensuring the security of critical elements and processes "by design" changes the security paradigm from reactive (bolted-on) to proactive, and fosters the development of a self-strengthening civil aviation system, therefore enabling it to evolve and enabling improved resilience in a more automated manner, where proven effective.

d) Align with other ICAO cybersecurity initiatives, coordinate with safety and security management provisions, and leverage existing initiatives. Existing ICAO groups of experts currently deal with various cybersecurity aspects. Potential lack of coordination of ongoing work might lead to inconsistencies, gaps and overlaps. It is therefore essential to ensure appropriate coordination among them all. Appropriate coordination amongst groups of experts dealing with cybersecurity issues is paramount to eliminate potential overlaps, inconsistencies or missing requirements. Of particular concern is ensuring that these expert groups have a mutual understanding of each other's objectives and work items in order to ensure the overall effectiveness and efficiency of ICAO's work on this subject matter and to optimize the use of the limited resources available. In this regard, cooperation procedures must be put in place by all stakeholders and existing ones should be enhanced to reflect the following principles:

- mutual understanding of objectives and vision;
- cooperative development;
- reciprocity;
- sharing of resources; and
- regularity.

3.1.3 It is imperative to ensure the comprehensive and coherent management of risks to civil aviation by coordinating safety and security management provisions. Annex 17 – *Security*, Annex 19 – *Safety Management* and other relevant cybersecurity risk management provisions need to be analyzed to ensure that no overlaps, gaps or inconsistencies exist. Cybersecurity must interface with other disciplines (safety, efficiency) similarly to what currently happens with "traditional" aviation security to ensure the accurate assessment of exposure to cybersecurity threats and ensure the development of effective and efficient risk-based cyber-protection strategies. Cybersecurity needs to build bridges between aviation security and safety as the multi-disciplinary nature of cybersecurity needs to benefit from:

- Security: the threat source profiling and identification of defensive measures (understand the threat sources and possible risk control measures); and
- Safety: Understanding of the civil aviation sector systems and operations (understand the vulnerability and attack paths, as well the consequences/effects of attacks that may jeopardize safety and continuity of operations).

3.1.4 Existing cybersecurity initiatives should be leveraged to promote the implementation of basic fundamental cybersecurity requirements. Many activities have been initiated either locally, regionally and/or globally to manage cybersecurity threats and risks. Some of them are specific to the civil aviation sector; and while some others are not, they are of significant value if tailored to civil aviation requirements, given that civil aviation cybersecurity has much in common with other industry sectors. As solutions need to be rapidly implemented to manage cyber-threats, there is a need to develop a complete inventory of these initiatives prior to embarking on specific work streams.

Chapter 4

STRATEGIC ACTION PLAN

4.1. THE SEVEN PILLARS OF THE CYBERSECURITY STRATEGY

4.1.1 The elements documented in this chapter have been developed with the aim to propose a series of principles, measures and actions to achieve the objectives of the Cybersecurity Strategy's seven pillars, namely:

1. International cooperation
2. Governance
3. Effective legislation and regulations
4. Cybersecurity Policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training and cybersecurity culture

PILLAR 1 - INTERNATIONAL COOPERATION
• Develop cooperation at the national and international level; • Recognize mutually the efforts (develop, maintain and improve cybersecurity) to protect civil aviation; • Achieve regulatory harmonization at the global, regional and national level in order to promote global coherence and ensure interoperability of protection measures; • Engage States in addressing cybersecurity in international civil aviation; • Facilitate and promote international events in the cybersecurity field.

PILLAR 2 - GOVERNANCE
• Encourage, support and build upon the ICAO Cybersecurity Strategy; • Develop clear national governance and accountability for civil aviation cybersecurity; • Ensure coordination at the State level between Civil Aviation authorities and the competent national authority for cybersecurity; • Establish appropriate coordination channels among various State authorities and industry; • Include cybersecurity in national civil aviation safety and security programmes; • Include cybersecurity in global and regional plans; • Work towards a common baseline for cybersecurity Standards and Recommended Practices.

PILLAR 3 - EFFECTIVE LEGISLATION AND REGULATIONS
• Ensure that international legal instruments provide appropriate measures for the prevention, prosecution and timely reaction to cyber-incidents; • Ensure that appropriate regulation and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and industry in implementing cybersecurity-related provisions.

PILLAR 4 - CYBERSECURITY POLICY
• Ensure that cybersecurity is a part of aviation security and safety systems and comprehensive risk management frameworks; • Ensure varying risk assessment methodologies retain comparability; • Develop cybersecurity policies considering the complete life cycle of aviation systems.

PILLAR 5 - INFORMATION SHARING
• Develop sharing of information platforms and mechanisms which are recognized, in line with existing ICAO provisions, to allow prevention, early detection and mitigation of relevant cybersecurity events.

PILLAR 6 - INCIDENT MANAGEMENT AND EMERGENCY PLANNING
• Ensure appropriate and scalable plans that provide for continuity of air transport during cyber incidents; • Encourage the use of existing contingency plans and include provisions for cybersecurity and for the conduct of exercises to test cyber resilience.

PILLAR 7 - CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE
• Ensure qualification of personnel in both aviation and cybersecurity; • Increase awareness of cybersecurity; • Ensure proper curricula on aviation cybersecurity are included in the national educational framework, in order to ensure the development of a cross aviation safety and security body of knowledge thought the organization including its senior management; • Foster cybersecurity innovation and appropriate research and design; • Include cybersecurity in the ICAO Next Generation of Aviation Professionals' strategy.

Chapter 5

IMPLEMENTATION, MONITORING AND REVIEW

5.1. IMPLEMENTATION

The CyAP is applicable to ICAO, its Member States, industry and other stakeholders. Each entity is encouraged to adopt the targets based on the Roadmap (see Appendix A), which outlines priority outcomes, actions and related tasks. This will help ICAO, States, and stakeholders focus and work towards implementing effective measures and actions to achieve the objective of developing a robust global cybersecurity framework.

5.2. MONITORING AND REVIEW

ICAO will conduct a review of the CyAP as and when appropriate. ICAO will also provide status updates for targets and intended deadlines as outlined in the CyAP. These will include areas where States need assistance with the implementation of the CyAP and/or where capacity-building assistance is needed, and other relevant efforts.

5.3. WORKING IN PARTNERSHIP

All aviation stakeholders need to be involved in the effort for the continuous improvement of cybersecurity in civil aviation. The CyAP provides a common frame of reference for all stakeholders and identifies actions that ICAO, Member States, and industry need to take in order for a common cybersecurity framework to be developed.

5.4. ROLE OF ICAO, STATES AND STAKEHOLDERS

5.4.1. ICAO will have an important global leadership and monitoring role in the implementation and coordination of the CyAP, including:

- updating the CyAP as and when required;
- developing and maintaining SARPs and PANS supplemented by manuals and other guidance;
- monitoring and reviewing the cybersecurity threat and risk landscape; and
- implementing targeted assistance to address deficiencies in the aviation cybersecurity system.

5.4.2. States and industry also have an important role to undertake in the implementation and effectiveness of CyAP. States and stakeholders are encouraged to demonstrate year on year improvement in the implementation of the plan.

Chapter 6

INTERNATIONAL COOPERATION[3]

6.1. DEVELOPMENT OF AN INVENTORY OF AVIATION CYBERSECURITY INITIATIVES

6.1.1. An inventory of cybersecurity initiatives will be developed, maintained and made available on the ICAO portal for appropriate audiences. This inventory will compile already existing initiatives and encompass existing aviation initiatives related to cybersecurity at the global, regional or national levels. The inventory will not only consider aviation cybersecurity initiatives but also initiatives whose outcomes are relevant to civil aviation (e.g. cybersecurity in other transport domains or sectors like energy, finance).

6.2. ESTABLISHMENT OF A COMMON GROUND FOR INTEROPERABILITY OF CYBERSECURITY MEASURES AND MANAGEMENT SYSTEMS[4]

6.2.1. Principles and appropriate tools/systems should be put in place by States and industry in order to assure uniform and interoperable management of information technology/communication systems.

6.2.2. As trust is the basis for effective, uniform and interoperable management of information technology/communication systems, it is necessary to develop a trust framework supporting a global effective, uniform and interoperable management of such systems. This trust framework should, among other elements, stem from types of trust such:

- trust according to attributes: based on identity and behaviour;
- trust according to the way it was obtained: either direct or through recommendation including the means utilized;
- trust according to certain roles: either defined by a certain code/procedure, third party, or trust in the means and ways of execution; and
- trust according to a subjective or objective evaluation.

6.2.3. Interoperability of cybersecurity measures and management can also be achieved by participation in various forms of international cooperation agreements. A model for such agreements should be developed in order to enable cooperation while respecting applicable privacy and national security policies. In this respect, the following aspects need to be determined as a baseline for model agreements:

- subject and objective of the agreement;
- measures that could be used by parties to improve cybersecurity in civil aviation and that are subject to coordination; and
- the entities that could enter into such agreements.

6.2.4. The international agreements should have, as their purpose:

[3] Actions related to this Chapter are reflected in Table 1 of Appendix A to the Action Plan.
[4] Management systems in this context include, but are not limited to, risk management systems.

- establishing a dialogue amongst stakeholders to discuss means to reduce collective risk and protect national and international civil aviation infrastructure;
- risk reduction and mitigation measures to address cybersecurity threats to civil aviation;
- information exchanges on national civil aviation legislation, national strategies, policies and best practices; and
- measures to support capacity building where needed.

6.2.5. In a context where many methodological principles and models, as well as a different vocabulary, may exist amongst aviation stakeholders, it is key to develop a common lexicon and frame of understanding. In this regard, a general set of principles for the appropriate, global and coordinated management of cybersecurity risks must be further developed at the ICAO level, in close cooperation with Member States and industry. An analysis of the existing framework will be conducted in order to determine the best way to achieve seamless and effective alignment of these principles and models.

6.3. DEVELOPMENT OF COMMON TERMINOLOGY

6.3.1. A common civil aviation cybersecurity-related terminology will be developed under the umbrella of ICAO, taking into account existing cybersecurity-related terminology and aviation-related terminology to allow all aviation stakeholders, whatever their background and activity level, to understand each other.

6.3.2. The aim is to facilitate cybersecurity-related activities. It does not mean that a single definition will be determined and/or agreed for all terms. It is acceptable that various definitions exist for the same term (e.g. likelihood, severity, occurrence etc.), provided that they are context-specific and that this repetition does not generate confusion that may cause ineffective management of civil aviation cybersecurity risks. Specifically, with an increased focus on integrated safety and security risk management, ICAO must pay very close attention to ensure terminology is aligned correctly. Recalling the initial context statement above, and the clarification between security in managing unlawful and intentional acts, and safety being concerned with intentional, non-intentional, and random hazards, this needs further refinement with respect to issues of integrated risk management which may span across both security and safety concerns (ICAO Annex 17 and Annex 19 definitions can be used as baselines). Specifically, with the differing focus of safety and security disciplines (with safety being concerned with intentional, non-intentional or random hazards and security concentrated on unlawful and intentional acts), the introduction of integrated risk management spanning across both disciplines requires clarity of scope and purpose of terms used.

6.4. DEVELOPMENT OF A GENERIC MAP OF INFORMATION EXCHANGE/INTERACTIONS IN AVIATION

6.4.1. A common framework for the identification of high-level functional maps describing the exchanges of information between all aviation actors is a necessary prerequisite to ensure understanding of the cyber-risk landscape. A common framework for identifying high-level mappings for information exchanges between all aviation stakeholders is needed to achieve an understanding of the cyber-risk landscape.

6.4.2. This high-level map of information exchange/interactions mapping should be generic enough to encompass all type of operations and should be, as much as possible, independent from the implemented physical and/or technical architectures (functional/service approach). For example, the high-level mapping should, as an example, cover digital data flows for air traffic management, airport-related

activities, and digital data flows for aircraft in flight/maintenance operations. This high-level map should leverage any existing efforts that have already been commenced by other groups. The purpose would be to allow each stakeholder to complete/adapt/customize their own map in regard to how it is interacting with other stakeholders. Ultimately, each stakeholder should be able to develop or adapt this mapping to their own unique situation. Accordingly, the results of the security risk assessments conducted by each actor using its own methodology and criteria (that have been made comparable based on a common risk assessment framework – see section 6.6) can be exchanged/shared with other stakeholders. By working together, using comparable security risk assessment frameworks and using the map of information exchange/interactions, stakeholders will be able to understand how risks can further propagate to or be managed by other risk-sharing partners, and therefore allow for the sharing of information about risks incurred or induced by each stakeholder.

6.5. DEVELOPMENT OF INTER-ORGANIZATION RISK INFORMATION SHARING

6.5.1. There are many standards and guidance documents which address the responsibility that each organization has for its own cybersecurity management, dealing with internal systems, processes, products and data. However, given that risks to civil aviation are shared between multiple stakeholders, there is a need to look beyond the individual organizations. To effectively and efficiently achieve shared risk management, sharing of risk information must be emphasised, which is inherent in conditions where systems, processes, products or data are shared, or are passed from one organization to another.

6.5.2. A standardized External Agreement which covers information security issues around an external interface and/or use of third-party products of which a number of examples currently exist should be explored as a possibility to develop a common basis for this type of sharing. The External Agreement concept requires sharing relevant security information about the interface or product to support the management or shared threats and risks across the supply chain.

6.6. DEFINE CRITERIA FOR RISK ASSESSMENT POSTURES COMPARABILITY

6.6.1. In a context of risks spanning across multiple organizations, it is essential that stakeholders can understand the end-to-end risks and the related risk-management posture of the other stakeholders for the management of these risks. In this context, criteria to enable the easy understanding and comparability of the risk assessments should be developed.

6.7. DEVELOPMENT OF APPROPRIATE CIVIL-MILITARY COORDINATION

6.7.1. Where possible and consistent with national security and national defence requirements, civil and military aviation interfaces should be interoperable, having due regard for national security and defence requirements such as confidentiality and security, and, whenever applicable and adequate, also be interoperable with the capabilities of other States.

6.7.2. Appropriate cybersecurity-related information-sharing and coordination between civil and military aviation stakeholders from an early stage can be highly beneficial to identify potential cyber-threats and thus contributes to successful mitigation of cyber-risks to the aviation system.

6.7.3. Information-sharing between civil and military aviation stakeholders is also important in the management of cybersecurity-related crises. States may offer support to their national civil aviation and military stakeholders in the organization of an arrangement to, as far as practicable, facilitate information-sharing through appropriate mechanisms.

6.8 PROMOTION OF GLOBAL AND REGIONAL EVENTS FOR CYBERSECURITY IN CIVIL AVIATION

6.8.1. ICAO will support and plan the organization of global and regional events to promote cybersecurity in civil aviation, as appropriate.

Chapter 7

GOVERNANCE

7.1 ICAO TO ESTABLISH A GOVERNANCE STRUCTURE

7.1.1. ICAO should establish a governance and accountability structure for aviation cybersecurity that includes appropriately skilled security, safety, resilience and operational continuity resources from States and industry (aviation and cybersecurity communities). This structure should comply with the criteria endorsed by the 40th Session of the ICAO Assembly.

7.2 DEVELOPMENT OF MULTI-ANNUAL PLAN(S) FOR CYBERSECURITY

7.2.1. It is recommended that the Cybersecurity Action Plan (CyAP) is properly aligned with the existing Global Aviation Security Plan (GASeP), Global Air Navigation Plan (GANP), and Global Aviation Safety Plan (GASP), and cybersecurity aspects should be included and promoted in these plans where appropriate.

7.3 DEVELOPMENT OF GOVERNANCE AND ACCOUNTABILITY

7.3.1. ICAO should develop cybersecurity policy guidance to facilitate harmonization and consistency amongst global, regional and national policies. National specific aspects ought to be justified and facilitate trans-national compliance.

7.3.2. States and organizations are encouraged to put in place an Information Security Management System (ISMS) with a common management approach and to identify specific cybersecurity roles and responsibilities in civil aviation. States should take tangible actions to continuously improve the efficiency, quality and consistency of the cybersecurity management processes at the national level.

7.3.3. Cybersecurity governance must be policy-driven and enforced, and accountability needs to be determined for compliance. Personnel should follow similar provisions as for security and safety management systems. A cybersecurity programme in civil aviation at the national level should be top-down to facilitate the processes and goals and ensure protocols are followed. Senior management should remain engaged throughout the lifecycle of the programme.[5]

[5] When developing cybersecurity governance at the national level, States may take inspiration from ISO 27001 to define leadership principles, such as : ensuring that information security management system requirements are integrated into the organizations processes; ensuring that the resources needed are available; and ensuring that the information security management system achieves its intended outcomes

Chapter 8

EFFECTIVE LEGISLATION AND REGULATIONAL FRAMEWORK

8.1 REVIEW OF EXISTING INTERNATIONAL AIR LAW INSTRUMENTS AS THEY PERTAIN TO THE CYBERSECURITY FIELD

8.1.1 ICAO will conduct an analysis of the existing international air law instruments to identify existing and potential missing provisions in relation to cyber threats and propose potential solutions to cover identified gaps with the purpose of further protecting civil aviation.

8.2 KEEPING ICAO PROVISIONS ALIGNED WITH CYBERSECURITY NEEDS

8.2.1. As cybersecurity in aviation matures, provisions may need to be developed to complement or supplement existing SARPs and PANS. This should be done on a case-by-case basis, noting that adding new provisions should be avoided to the maximum extent possible and, where necessary, coordinated amongst all relevant expert groups.

8.3 RATIFICATION OF THE BEIJING CONVENTION AND PROTOCOL

8.3.1 States are encouraged to ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention 2010) and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol 2010).

8.4 STATES TO ENSURE APPROPRIATE LEGISLATION AND REGULATIONS ARE FORMULATED AND APPLIED AT THE NATIONAL LEVEL

8.4.1. States are encouraged to evaluate their existing national legal frameworks in the field of cybersecurity and civil aviation in order to determine existing gaps as well as to ensure appropriate legislation is in place for specific civil aviation cybersecurity elements. Another key component is the enforcement mechanism that States are encouraged to implement for the criminalization and prosecution of unlawful cyber acts against civil aviation.

Chapter 9

CYBERSECURITY POLICY

9.1. ELABORATE AND IMPLEMENT CYBERSECURITY POLICIES

9.1.1. Along with the set of policies associated for civil aviation-specific cybersecurity risk management, Guidance Material to support effective implementation of ISMS should be developed at the global, regional and national levels.

9.1.2. This guidance could be built upon already available guidance documents:

- to assist in defining the scope to which the ISMS is applied;
- for self-assessment of current status;
- to define maturity targets; and
- develop a plan to achieve the maturity target.

9.1.3. A cybersecurity policy needs to be developed at national and organizational levels. States should have in place criteria for the establishment of a clear and actionable cybersecurity policy that includes:

- objectives stemming from results of the civil aviation cybersecurity risks assessments;
- a commitment to satisfy applicable requirements and the way to assess compliance;
- considerations related to the management of and coordination with external dependent parties (ref. to international collaboration chapter);
- a commitment to continuous improvement of information security management;
- provisions to ensure that the policy is fully documented and is available as official information; and
- provisions to ensure that the policy is properly disseminated.

9.2. IDENTIFY AND EVALUATE CYBER-RISKS TO CIVIL AVIATION

9.2.1. One of the challenges of risk identification and evaluation activities is to be able to anticipate the rapid changes in the sources of threats. Anticipation of changing threats is key to help the air transport system proactively adapt its protection strategy not only according to current threats, but also in light of potential future threats. Thanks to this anticipation, the civil aviation sector should be able to be more proactive in a context whereas there is asymmetry between agility of the attackers that are very agile and adaptive and the defenders that, given the complexity of the system to be protected, are slow to react. In this scenario, this proactive approach becomes even more critical. Hence, it is necessary to develop a cybersecurity risk identification and evaluation framework supporting this need, to help mitigate these risks.

9.2.2. It is recommended that cybersecurity risks be identified and assessed taking into account all the potential consequences of an attack on the civil aviation system (security, safety, resilience, continuity of service, etc.), as well as all potential sources of threat. This activity should build on the cyber-risk matrices previously developed under the auspices of the Aviation Security Panel Working Group on Threat and Risk (WGTR).

9.2.3. Since a significant proportion of cybersecurity risks for civil aviation are shared by many stakeholders, it is recommended to consider the mapping of information exchanges/interactions in aviation (see Chapter 6.1). This mapping should be used as a means of guaranteeing the exhaustiveness of the scenarios considered and to enable stakeholders to understand how they interact with each other and their dependencies on risks.

9.2.4. It will not be feasible to assess risks for all possible scenarios that may exist around the world. It is therefore necessary to consider a generic civil aviation cybersecurity architectural and operational framework that will make it possible to enable identification and assessment of generic risks. These generic risks will have to be reworked, if necessary, on a case-by-case basis and can then be tailored as needed by civil aviation stakeholders, taking into account their specific system infrastructure and operational requirements. In order to enable them to understand the context of generic risk analyses and to help them adapt the results of the risk assessment to their specificities, all assumptions in the modeled generic risks framework should be fully documented.

9.2.5. As the level of severity of cybersecurity risks will vary over time (i.e. these risks can evolve rapidly compared to others), it is recommended to consider a means to adapt any global aviation response to these risks that can be deployed in a rapid and coherent manner (e.g. balancing the need for aviation standards, guidance materials, non-aviation best practices, and using/relying on other domain responses).

9.2.6. It is recommended that the identification and evaluation of generic cybersecurity risks be entirely carried out and coordinated by a group of experts composed of civil aviation cybersecurity experts, or, failing that, by a team of cyber and civil aviation experts, preferably with an extensive background in cybersecurity.

9.2.7. This group of experts should be responsible for the development of a Cyber Risk Context Statement complementing or adding to the existing Doc 10108 with cybersecurity aspects.

9.2.8. The group of experts should work closely with WGTR and other expert groups as needed to ensure that any gaps, overlaps or inconsistencies are avoided when assessing cybersecurity risks, and that recommendations are aligned with AVSECP and other expert group recommendations where appropriate.

Chapter 10

INFORMATION SHARING

Sharing of information serving the management of the security is essential to the defence of the civil aviation systems and to furthering cybersecurity. In recognition that promoting information sharing is a key element of building cybersecurity culture, civil aviation stakeholders should develop and implement programmes enabling the sharing of information within their organizations and with external parties. Through these programmes, they should develop partnerships and share substantive information with other stakeholders which own and operate civil aviation infrastructure, and develop information-sharing schemes and practices within their organizations.

These information-sharing programmes should enable the development, operation and adjustment of civil aviation defence against known and emerging security threats. They should help develop:

- Situational awareness in both normal day-to-day operations, and during a crisis or event;
- Operational and tactical risk management in anticipation of, and response to a threat;
- Strategic planning to build capabilities that strengthen cyber-security and resilience for the future.

10.1. DEVELOPMENT OF RISK INFORMATION SHARING

10.1.1. Sharing cyber-related information has bi-lateral and multi-lateral dimensions – any combination amongst and across (nationally, regionally, globally) the following parties:

- national cyber authorities;
- national civil aviation authorities;
- national military aviation authorities;
- other aviation stakeholders (operators, service providers and manufacturers); and
- non-aviation stakeholders (IT and communications providers and supply chain).

10.1.2. It is recognized that there are many types of cybersecurity-related information, such as:

- *Cyber-intelligence* - (threat landscape, intelligence about cyber threat actors' capability and intent): this can be sensitive and there can be restrictions (Traffic Light Protocol or TLP markings can help with sharing to some extent).

- *Indicators of Compromise (IoCs)* - these can be shared as they are not related to individual systems/services (TLP (Traffic Light Protocol) still to be used). IoCs are e.g. malicious IP, malicious URL, Malware hash. Sharing this information will help others protect themselves; similarly, receiving this information from others will help entities better protect their systems/services. There is no need to further disclose who has discovered them (be it ANSP A or ANSP B or Airport Operator C or Airport Operator D or Airspace User E or Airspace User F, etc…) as it does not add any value.

- *Tactics, Techniques and Procedures (TTPs)* - (scenarios of attacks, preferred methods used by hackers): this information can be shared (TLP still to be used) as it is usually not related to particular systems/services.

- *Vulnerabilities,* only relevant information should be shared about the vulnerability (hardware, software, service, protocol, standard, etc.) including potential exploit scenarios, and not who may be using it.

- *Incident reports* - TLP and de-identification can be used to share some incidents, while some incidents may be excluded from sharing.
  a) serious incidents: National/Regional mandatory reporting (e.g. as per general cybersecurity and data protection regulations such as the European Union General Data Protection Regulation – GDPR, or Critical Infrastructures National or Regional regulations e.g. NIS Directive) may be shared; and

  b) non-serious incidents and near-incidents: can be shared (de-identified).

10.1.3. Depending on national legislation and the nature of the cyber-related information, there could be various methods and constraints to share the information with various recipients (e.g. national cyber authority, national civil aviation authority, national military aviation authority, and other aviation stakeholders).

10.1.4. Information-sharing, collaboration needs (including but not limited to times of crisis), and policies should be identified at the global, regional and national levels.

10.1.5. It is recommended to use TLP to state the level of distribution/restrictions when distributing and further sharing cyber-related information. (See Appendix B).

10.1.6. The vast majority of cyber-related information can be shared without using an information classification system (e.g. confidential/secret/top secret). Using such systems should remain the exception rather than the rule.

10.1.7 Cyber-related information, which may contain some sensitive information, should be de-identified or sanitized before sharing, rather than not sharing it at all.

10.2. DEVELOPMENT OF PRINCIPLES AND GUIDANCE FOR SECURITY RESEARCHER RESPONSIBLE DISCLOSURE

10.2.1 Given the growing interest of the security researchers' community in civil aviation cybersecurity, and to avoid irresponsible disclosure of potential findings that may be detrimental to civil aviation, principles for the responsible disclosure of vulnerabilities discovered by researchers, or third parties, need to be defined to ensure that disclosures are not detrimental to civil aviation cybersecurity. This should take into consideration recommendation 4.4 of the Cybersecurity Strategy.

10.2.2. Guidance for these principles (addressing, amongst other concerns, e.g. discovery, notification, investigation, resolution and release) should be established between, on one hand, researchers and third parties, and on the other hand, aviation authorities and aviation stakeholders to ensure, to the maximum extent possible, that such vulnerability research/discovery and disclosure activities have no impact on safety and service provision. Ideally guidance would not only address responsible disclosure processes, but also include awareness and educational elements.

10.3. DEVELOPMENT OF A GLOBAL NETWORK OF REGIONAL/NATIONAL CYBER AUTHORITIES FOR CIVIL AVIATION PURPOSES

10.3.1. Cybersecurity responsibility within States and industry is not uniformly assigned, and appropriate expertise is spread across a wide range of external stakeholders and functional areas. The innate concern of this variety creates difficulty in identifying the appropriate point of contact within an entity, and establishment and maintenance of formalized communication channels between stakeholders. Guidance on establishing and maintaining a single point of contact for civil aviation cybersecurity-related matters within States and organizations can facilitate the building of global, regional and national communication channels, build appropriate cybersecurity communities, and drive cybersecurity culture.

10.4. GLOBAL CYBERSECURITY INFORMATION SHARING CAPABILITY FOR AVIATION

10.4.1. Civil aviation information-sharing capabilities may be developed transversely at the global, regional, and/or national levels to foster the exchange of cybersecurity-related information.

Chapter 11

INCIDENT MANAGEMENT AND EMERGENCY PLANNING

11.1. DEVELOPMENT OF INCIDENT RESPONSE CAPABILITIES AND EMERGENCY RESPONSE PLANNING

11.1.1. All stakeholders are strongly encouraged to develop and test incident response and emergency plans in a coordinated manner with their operational partners, which includes:

- making use of existing contingency plans that are already developed and/or amending these plans to include provisions for cybersecurity;
- that civil aviation stakeholders develop and maintain appropriate scalability that provides for the continuity of air transport operations during possible cyber incidents;
- development of provisions for cybersecurity incident response and recovery capabilities, including contingency and emergency response plans;
- involving military aviation stakeholders in the planning process, to proactively establish lines of communication;
- achieving acceptable performance levels and satisfying the requirements to maintain minimum service levels of essential services; and
- coordinating civil aviation and cyber security incident reporting schemes at national, regional, and, where available, international levels.

11.2. INCIDENT DETECTION, ANALYSIS AND RESPONSE MEANS AT THE STAKEHOLDER LEVEL

11.2.1. To the extent possible, incident response plans should be implemented, and stakeholders should develop the capabilities for cybersecurity incident detection, analysis and response at all levels. It is important to monitor the cybersecurity status of those systems/services as deemed critical in supporting civil aviation, in order to detect potential problems and to track the ongoing effectiveness of protective security measures. Once detected, cybersecurity incidents should be analysed and appropriate response plans put into action; these should include mitigating actions to limit the impact of the cybersecurity incident.

11.3. DEVELOPMENT OF A CRISIS COORDINATION CELL FOR CIVIL AVIATION

11.3.1. A civil aviation crisis coordination cell embedding civil aviation cybersecurity expertise should be implemented when possible (building on already existing mechanisms) and, where appropriate, military aviation stakeholders should be involved.

11.3.2. Periodic exercises should be conducted regularly, in particular table top exercises (TTX) based on real incidents, with industry participation from all relevant stakeholders.

Chapter 12

CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE AND EDUCATION

12.1. DEVELOPMENT OF TECHNICAL CAPACITY, TRAINING AND CYBERSECURITY CULTURE AND EDUCATIONAL MATERIAL

12.1.1. Education, training and awareness on civil aviation cybersecurity should be defined and promoted at the global, regional, and national levels.

12.1.2 Cybersecurity culture and educational activities should be promoted from the senior management level throughout civil aviation organizations, and should highlight the key roles of and expectations from the different actors. It should lead to the development of a cross aviation safety and aviation security cybersecurity body of knowledge, and should include:

- notions of secure-by-design principles to mitigate cyber threats, in coordination with the safety community. These notions should help the aviation safety community make better-informed decisions when addressing cyber threats;
- coordinated approach between security and safety stakeholders, recognizing that security controls must not have a negative impact on safety of flight, enabling the transfer of technical knowledge ensuring that informed decisions are taken on the basis of a mutually understood risk landscape;
- notions of cyber hygiene practices for operational and support staff that should help prevent potential adverse impacts to the civil aviation system caused by the increasing number of "Commercial Off the Shelf" (COTS) products and non-specific malware; and
- notions of "Just Culture" from the safety community to enable and stimulate self-reporting of occurrences that results from unintended behaviour by personnel (e.g. unintentional malpractice in handling an USB Stick)

12.1.3 In carrying out these activities, emphasis should be placed on impact or potential impact.

12.1.4 The development of this cybersecurity culture and promotion of cybersecurity culture and educational material should help develop a mutual/common understanding in security and safety communities of the cybersecurity risk landscape, as well as a mutual confidence in the countermeasures being put in place.

12.1.5 ICAO should encourage trans-national/trans-regional exchange programmes on cybersecurity education and training. [6]

12.1.6 Cybersecurity culture and education activities should not only focus on systems operation but rather on their entire system life-cycle, including:

[6] As for example initiatives for multinational campus or EU Cybersecurity Competence network and centres.

- design (security for hardware, software and data, change management, vulnerability management);
- manufacturing/acquisition (including industrial supply-chain);
- operation (including access management, data integrity, secure systems operation);
- maintenance (including patching and update strategy); and
- disposal (including management of credentials and residual data on storage devices).

Chapter 13

CONCLUSION

The Cybersecurity Action Plan will bring together ICAO, States, industry, and other stakeholders in a holistic and coordinated effort to address current and emerging cybersecurity challenges. It will also highlight that cybersecurity is a cross-cutting issue that involves all domains of the aviation sector. The plan will assist ICAO, States, industry, and other stakeholders in fulfilling their obligations deriving from the ICAO Cybersecurity Strategy towards creating a robust global cybersecurity framework.

— — — — — — — —

APPENDIX A

Cybersecurity Action Plan Roadmap

CYBERSECURITY STRATEGY GENERAL ACTIONS

Priority Outcome		**DEVELOP A GLOBAL AND AGREED VISION**			
Priority Actions		• Recognize that it is imperative to develop a comprehensive and agreed cybersecurity vision as a foundation to solid and coordinated global aviation cybersecurity risk management; • Recognize that the civil aviation sector shall be resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow; • Recognize that cybersecurity risks are to be treated under the convention on International Civil Aviation.			
Actions					
Action #	**By**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 0.1	ICAO	ICAO to develop a Cybersecurity Policy Statement Model at international level. Member States and Industry to develop such policy statement model at national and organizational level.	The model is available to States and Industry		2020
CyAP 0.2	ICAO and Member States	Commence the implementation work of the ICAO Cybersecurity Strategy at national level (as instructed in Resolution A40-10) (in order to verify how States implement the Strategy a set of metrics need to be developed to measure the implementation of certain actions)	National evidence of commencement of implementation work		2021
CyAP 0.3	ICAO	Conduct surveys to establish how States have implemented the ICAO Cybersecurity Strategy. (survey to ask if States have developed an action plan to implement the Strategy).	ICAO survey/questionnaire sent to the Member States		2022

CYBERSECURITY STRATEGY PILLARS

Priority Outcome	**1. ACHIEVE INTERNATIONAL COOPERATION**
Priority Actions	• Develop cooperation at national and international levels; • Mutual recognition of the efforts (develop, maintain and improve cybersecurity) to protect civil aviation; • Achieve regulatory harmonization at global, regional and national level in order to promote global coherence and ensure interoperability of protection measures; • Engage States in addressing cybersecurity in international civil aviation; • Facilitate and promote international events in the cybersecurity field.

Actions							
Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 1.1	ICAO	1.1.	6.2	Include Cybersecurity in ICAO safety and security oversight programmes – include relevant Standards in the ICAO audit programmes (such as USOAP and USAP)	ICAO audit programmes from both safety and security perspectives include Cybersecurity relevant Standards.	N/A	Ongoing
CyAP 1.2	ICAO	1.1.	6.1 See also CyAP 4.7 (Para 9.2 Action Plan)	Conduct surveys to list the cybersecurity initiatives/practices to establish how States and industry are managing civil aviation cybersecurity	Results of questionnaires, number of initiatives and regions.	N/A	Ongoing
CyAP 1.3	ICAO	1.1	6.1	Develop an inventory of all the cyber-security initiatives engaged in the different ICAO supporting groups of experts			2020

CyAP 1.4	ICAO	1.2	6.2.3 and 6.5 See also CyAP 5.1 (Para 10.2 Action Plan)	A) Develop models of Memoranda of Understanding/ Collaboration, External Agreements B) Provide guidelines on how to develop/introduce/review these agreements.	Availability of template and guidelines	N/A	2022 - 2023
CyAP 1.5	ICAO	1.2	6.5	A) Develop models for External Agreements linked to shared risks management B) Provide guidelines on how to develop these agreements.			
CyAP 1.6	ICAO	1.2	6.3	Develop a common and agreed civil aviation cybersecurity related terminology to allow all aviation stakeholders, whatever their background and activity level, to understand each other with regards to cybersecurity.	Publication of a comprehensive cybersecurity glossary	N/A	2021
CyAP 1.7	ICAO, Member States, and Industry	1.2	6.4	ICAO to develop a common framework for the identification of high-level functional map describing the exchanges of information between aviation actors (e.g. ANSP, AOC, A/C, Airport, MET, MRO, CNS.) as a necessary condition to ensure understanding of the cyber-risk landscape. Member States and Industry to develop such framework at national and organizational levela.	Existence of common framework and identified generic map of information exchanges/interactions in aviation. Awareness and understanding of the functional map.	High	2022

CyAP 1.8	ICAO and Member States to cooperate when appropriate	1.2	6.7 See also CyAp 6.2 and Para 11.2 of the Action Plan)	ICAO to establish models of cooperation between civil and military aviation in order to develop, where appropriate, models/guidance for civil and military interoperable aviation interfaces. Determine criteria and level of appropriate interaction. Member States should cooperate with ICAO when appropriate.	Proof of such Availability of models/guidance for civil/military cyber cooperation and interoperability List of criteria and minimal required interactions publishedn.	High	2021
CyAP 1.9	ICAO, Member States and Industry	1.3	6.8	ICAO, with support from Member States and Industry, to plan, organize and support international and regional events to promote cybersecurity in civil aviation.	Events,Awareness building, international cooperation.	N/A	report by 2022 to Assembly
CyAP 1.10	ICAO, Member States, and Industry	1.3	6.4	Ensure that all relevant stakeholders are engaged in discussions and activities regarding cybersecurity in civil aviation: Continuous involvement and outreach with relevant stakeholders	Publish results of common efforts Publish proof of engagement such as partnerships, group membership, etc.	Low	ongoing
CyAP 1.11	ICAO	1.3	6.2	ICAO to ensure Member States include cybersecurity in their national civil aviation safety and security programmes.	ICAO Survey - Number of States that have included cybersecurity in their national aviation safety and security programmes	N/A	Survey 2020 Further actions ongoing
CyAP 1.12	ICAO, Member States, and Industry	1.2	6.2.2	Develop an international aviation trust framework that allow entities to interoperate according to the trust they have in other stakeholders	Establishment of a trust framework used by many organizations.	High	2022-2023
Priority Outcome	**2. DEVELOP GOVERNANCE AND ACCOUNTABILITY**						

Priority Actions	• Encourage, support and build upon the ICAO Cybersecurity Strategy; • Develop clear national governance and accountability for civil aviation cybersecurity; • Ensure coordination at State level between Civil Aviation authorities and competent national authorities for cybersecurity; • Establish appropriate coordination channels among various State authorities and Industry; • Include cybersecurity in national civil aviation safety and security programmes; • Include cybersecurity in global and regional plans; • Work towards a common baseline for cybersecurity Standards and Recommended Practices.

Actions

Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 2.1	ICAO		7.1	Establish a governance structure in the cybersecurity field	Identification of the most appropriate governance structure for cybersecurity	**N/A**	2021
CyAP 2.2	ICAO	2.2	7.3	ICAO to develop general set of principles on the appropriate management system for cybersecurity. Member States to develop such principles at national level following the ICAO model.	Publication of general principles	Medium	2022-2023
CyAP 2.3	ICAO, Member States, and Industry	2.2	7.3.2 See also para 9.1. of the Action Plan	Develop guidance material to support organizations in implementing coordinated ISMS and assessing ISMS maturity and effectiveness.	Publication of guidelines	Medium	2021
CyAP 2.4	ICAO and Member States	2.2	7.3	Promote coordination mechanisms between civil aviation authorities and cybersecurity ones	ICAO Survey – number of identified existing coordination mechanisms in place.	Medium	2020

CyAP 2.5	ICAO	2.3	7.2.1 See also CyAP 1.10 (Para 6.2 Action Plan)	ICAO to include cybersecurity in regional and global plans	Updated Plans published	N/A	2022-2023
CyAP 2.6	ICAO		7.2	ICAO to prepare best practices registry/guidelines section in the repository.	ICAO Repository of best practices	N/A	2020-2021
CyAP 2.7	Member States	3.2	7.3, 6.2	Develop criteria and checklists to include cybersecurity in audit programmes.	Development of criteria and checklists. Inclusion of cybersecurity in States aviation security and safety oversight policies.	High	2022 - 2023
CyAP 2.8	ICAO, Member States and Industry	3.2	7.3	ICAO to develop model procedures to report cyber incidents. Member States and Industry to develop national and organizational procedures to report cyber incidents	Cyber incidents reporting procedures / number of reported incidents according to the procedures	High	2022 - 2023

Priority Outcome	**3. DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS**
Priority Actions	• Ensure that appropriate regulation and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and Industry in implementing cybersecurity related provisions; • Ensure that international legal instruments provide appropriate measure for the prevention, timely reaction to, and prosecution of cyber-incidents.

Actions							
Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 3.1	Member States	3.3	8.4	Member States to ratify Beijing instruments.	Number of States having ratified Beijing instruments	Low	ongoing
CyAP 3.2	ICAO	3.3	8.3	Analysis of international air law instruments	Report and update plan	N/A	2020
CyAP 3.3	ICAO and Member States	3.3	8.2	Analysis of existing international and national legislation in the cybersecurity field and identify gaps, including criminal law.	Promote ratification of instruments to incriminate unlawful cyber acts.	Medium	2022 - 2023
CyAP 3.4	ICAO, Member States and Industry	3.3	8.1	Review existing ICAO security standards to identify need for potential cybersecurity updates	Regulatory gap analysis	High	2021
CyAP 3.5	ICAO	3.2	5.4	Create, review and amend guidance material related to implementing cybersecurity requirements	Accepted and agreed cybersecurity guidance material	High	2021-2022

Priority Outcome	**4. DEVELOP A CYBERSECURITY POLICY**						
Priority Actions	• Ensure that cybersecurity is part of the aviation security and safety systems and the comprehensive risk management framework; • Ensure varying risk assessment methodologies to retain comparability; • Develop cybersecurity policies considering the complete life cycle of aviation systems.						
Actions							
Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 4.1	ICAO, Member States, and Industry	4.1	9.1	ICAO to develop a cybersecurity policy (using the model developed by ICAO as per action CyAP0.1) to facilitate compliance of national policies with global and regional ones. National specific aspects should be justified and should facilitate trans-national compliance. Member States and Industry to develop national and organizational policies. Development of capacity building activities	Development of capacity building activities ICAO survey about Member States' Cybersecurity policy publication	Low	2022-2023
CyAP 4.2	Member States and Industry	4.1.	9.1	Senior management of organizations to be committed to and to support their organisations' cybersecurity efforts Member States (national aviation authorities) and Industry to ensure commitment of their management.	Awareness campaign / Proof of commitment such as declarations of commitment, defined responsibilities in the cybersecurity field in the management manuals of authorities and organizations	Medium	2022-2023

CyAP 4.3	ICAO, Member States, and Industry	4.3	9.2 See also para 6.11 Action Plan	Promote cybersecurity Research & Development in civil aviation by engaging with universities, institutes, researcher communities etc.	Number of interactions and projects	High	2022 - 2023
CyAP 4.4	ICAO, Member States, and Industry	4.2.	6.6 and 9.2	Define criteria for a shared trans-organizational risk assessment along with the information to be shared and the needed criteria for risk comparability will be developed by ICAO. Member States to define such criteria at national level, and the Industry at organizational level.	Publication of objectives and criteria for a shared trans-organizational risk assessment	High	2022
CyAP 4.5	ICAO, Member States, and Industry	4.3	9.1	Develop a policy for security by design as a basis for a secure life-cycle of aviation systems	Policy for secure life-cycle of aviation systems formulated	Medium	2022 - 2023
CyAP 4.6	ICAO, Member States, and Industry	4.2.	9.2	ICAO to develop international forums to discuss trans-organizational/trans-functional security and resilience targets and minimum level of functionalities essential to the civil aviation sector. Member States to develop such forums at national and regional level, and the Industry to develop specific forums and be actively involved in the forums established by ICAO and Member States.	Number of fora to discuss targets	High	2022 - 2023
CyAP 4.7	ICAO, Member States, and Industry	4.3	9.2	Establish an inventory of existing civil aviation cybersecurity risk management initiatives (risk profiles, scenarios, vulnerability management, and risk assessments).	Availability of a cybersecurity risk management initiatives' repository	Medium	2020

CyAP 4.8	ICAO, Member States, and Industry	4.3	9.3	ICAO to develop a list of strategic cyber risk scenarios at international level. Member States and Industry to contribute and develop similar lists at national and organizational levels.	Availability of 10 cyber risk scenarios to support CyAP 4.7	High	2022 - 2023
CyAP 4.9	ICAO, Member States, and Industry		9.2	ICAO to develop risk profiles for each operational domain. Member States and Industry to contribute by developing similar risk profiles at national and organizational levels.	Availability of risk profiles	High	2022
CyAP 4.10	ICAO		9.2	Develop a cybersecurity threat and risk register to complement WGTR RCS with a cybersecurity view beyond terrorism even if it is a theoretical threat and risk registry.	Availability of a cybersecurity threat and risk register	N/A	2020

Priority Outcome		**5. DEVELOP INFORMATION SHARING CAPABILITIES**					
Priority Actions		• Develop information sharing platforms and mechanisms, in line with existing ICAO provisions, to allow prevention, early detection and mitigation of relevant cybersecurity events.					
Actions							
Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 5.1	ICAO and Member States	**5**	10.2 See also CyAP 1.3 (Para 6.5 Action Plan)	ICAO to explore the concept of a standardized External Agreement and develop an ICAO model of such agreement as per action CyAP1.3, which covers the information security issues, around an external interface and/or use of third-party products. Member States, following the ICAO model, to develop national model agreements. Develop an External Agreement Model if deemed appropriate.	Template is published.	High	2022 - 2023
CyAP 5.2	ICAO, Member States, and Industry	5.1.	10.1 10.2	ICAO, with support of Member States and Industry, to develop guidance for information sharing.	Guidance document for information sharing available to the community.	High	2022 - 2023
CyAP 5.3	ICAO, Member States, and Industry	5.1.	10.1	ICAO, with support of the Member States and Industry, to identify cybersecurity related information sharing, collaboration needs (including but not limited to times of crises), and policies.	Develop a list of potential information to be shared	N/A	2020-2023
CyAP 5.4	ICAO, Member States, and Industry	5.1.	10.1	Use TLP (Traffic Light Protocol) to state the level of distribution/restrictions when distributing and further sharing cyber-information.	Publish policy Guidance for the use of TLP when distributing and sharing cyber information.	High	2020

CyAP 5.5	ICAO, Member States, and Industry	5.2.	10.2	Define principles for the responsible disclosure of vulnerabilities.	Availability and distribution of principles for the responsible disclosure of vulnerabilities.	High	2020
CyAP 5.6	ICAO, Member States, and Industry	5.2	10.4	ICAO to develop and maintain a point of contact network at international level for cybersecurity related matters for Member States and Industry. Member States to cooperate with ICAO by developing such network at national levels.	Establishment of a cybersecurity network. Publish the network point of contact.	Medium	2021-2023

Priority Outcome	**6. DEVELOP INCIDENT MANAGEMENT AND EMERGENCY PLANNING**

Priority Actions		• Ensure appropriate and scalable plans that provide for continuity of air transport during cyber incidents; • Encourage the use of existing contingency plans and include provisions for cybersecurity and conduct exercises to test cyber resilience.					
Actions							
Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 6.1	Member States establish targets Industry apply targets	6.1.	11.1	Member States to establish targets and minima levels of functionalities essential to the civil aviation sector. Industry to apply the targets developed (as per action CyAP4.6).	Publish a list of targets and minimal acceptable levels for aviation continuity	High	2022 - 2023
CyAP 6.2	ICAO and Member States	6.1.	11.2	ICAO to develop guidance and processes to include military stakeholders in cybersecurity incident response planning for civil aviation. Member States to develop procedures and cooperation agreements between civil and military aviation authorities.	Definition of civil-military cooperation processes in cybersecurity incident response	High	2022-2023
CyAP 6.3	ICAO, Member States, and Industry	6.1.	11.1	ICAO to develop guidance for cyber-incident response and recovery capabilities including contingency and emergency response plans. Member States and Industry, following the ICAO model, to develop such guidance at national and organizational levels.	Publish guidance for cyber-incident response and recovery capabilities including contingency and emergency response plans.	High	2022 - 2023
CyAP 6.4	Member States	6.1.	11.2 and 11.3	Member States to develop guidance and implement capability and plans for cybersecurity incident detection, analysis and response at operational level, in order to conduct oversight of the industry activity.	Study on the level or maturity of readiness of the plan	High	2026

CyAP 6.5	Member States	6.1.	11.1	Develop processes for civil aviation cybersecurity crisis coordination, including at national and international levels.	Definition of cybersecurity crisis coordination process established Template of process delivered	Medium	2022 –– 2023
CyAP6.6	Member States and Industry	6.1	11.3	Conduct periodically table top exercises (TTX) based on real incidents	TTX lessons learned	High	2022-2023

Priority Outcome	**7. DEVELOP CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE**

Priority Actions	• Ensure qualification of personnel in both aviation and cybersecurity; • Increase awareness about cybersecurity; • Ensure proper curricula on aviation cybersecurity is included in the national educational framework at professional development level, in order to ensure the development of a cross aviation safety and security body of knowledge from senior management thought the organization ; • Foster cybersecurity innovation and appropriate research and design; • Include cybersecurity in the ICAO Next Generation of Aviation Professionals' strategy.						
Actions							
Action #	**By**	**Traceability to the Cybersecurity Strategy**	**Traceability in Action Plan**	**Specific Measures/Tasks**	**Indicators**	**Maturity**	**Target**
CyAP 7.1	ICAO, Member States, and Industry	7.1.	12.1	Define and promote a civil aviation cybersecurity culture and education.	Availability of courses and guidance material related to civil aviation cybersecurity culture.	Medium	2022-2023
CyAP 7.2	ICAO, Member States, and Industry	7.2.	12.1	ICAO to identify gaps in existing aviation jobs to appropriately address cybersecurity concerns, and develop guidance as well as specific training. Member States and Industry to develop training requirements at all levels within their organizations.	Develop appropriate job related training.	High	2022 - 2023
CyAP 7.3	ICAO and Member States	7.3.	12.1	ICAO to include cybersecurity in the NGAP strategy. Member States, following ICAO, to include cybersecurity in their national strategies related to the Next Generation of Aviation Professionals' strategy.	Cybersecurity included in NGAP	Medium	2022-2023
CyAP 7.4	ICAO, Member States, and Industry	7.3.	12.1	Analyse means and ways to develop role-based competency requirements. ICAO to create a working group with the scope to develop such requirements. Member States and Industry to engage in this working group and to develop	Cybersecurity included in ICAO Doc 7192 and 9868	High	2022-2023

				competency requirements at national and organizational levels.			

———————

APPENDIX B

Definition of Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) is a method for someone sharing information to inform their audience about any limitations in further spreading this information.

The Traffic Light Protocol (TLP) was created and used since 2000 by the UK Government's National Infrastructure Security Coordination Centre (NISCC, now Centre for Protection of National Infrastructure – CPNI)

TLP provides an element for indicating when and how sensitive information can be shared, and for facilitating more frequent and effective collaboration. It is widely used in organizations such as CERTs, CSIRTs, and ISACs.

Other elements could be used to complement the use of TLP such as the Chatham House Rule, Common Vulnerability Scoring System (CVSS), and FIRST Information Exchange Policy (IEP). The TLP is in principle easy to use: the sharer of information tags the information with a colour. Tagging information consists simply of adding "TLP: COLOUR" on a document or part of it. The meaning of the colour indicates the possibilities for further spreading of the information. Over the years, different wordings of the TLP have surfaced, but the CSIRT community recently made an effort to clarify the TLP.

COLOUR	MEANING	EXAMPLE
RED	Not for disclosure, restricted to participants only. Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP: RED information with any party outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present in the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.	Information shared with people in a meeting; direct email.
AMBER	Limited disclosure, restricted to participants' organizations. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share	Sharing of Indicators of Compromise (IoCs) to an organisation's CSIRT. These could be forwarded to the SOC for further action.

COLOUR	MEANING	EXAMPLE
	TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.	
GREEN	Limited disclosure, restricted to the community. Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.	Sharing of a malware analysis with a specific industry sector.
WHITE	Disclosure is not limited. Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.	Public security advisory.

— END —