International Civil Aviation Organization

MIDANPIRG/23 & RASG-MID/13 Meetings

(Cairo, Egypt, 14 – 18 June 2026)

Agenda Item 5.7: CNS

CYBERSECURITY

(Presented by the Secretariat)

SUMMARY

This paper presents the actions undertaken by the MID Regional Aviation Security and Facilitation Group (MID-RASFG) in relation to Cybersecurity, including the development and analysis of the Cybersecurity Action Plan (CyAP) questionnaire, as well as the Conclusion proposing the establishment of a Regional multidisciplinary Aviation Cybersecurity Task Force.

Action by the meeting is at paragraph 3

REFERENCE

- ICAO Cybersecurity Action Plan
- MIDANPIRG/20 Report
- ICAO MID RAFIT/5 Report (3 - 5 February 2026, Doha, Qatar)
- CNS SG/15 Report

1. INTRODUCTION

1.1 The amendment 12 of the Annex 17 (effective 2011) included provisions to further strengthen Standards and Recommended Practices in order to address new and emerging threats to civil aviation, including the security of air traffic service providers. The air traffic management security is part of Aviation Security, and it’s a national responsibility.

1.2 The ICAO Assembly Resolution A40-10 requested ICAO to develop an action plan to support States and industry in the adoption of the Aviation Cybersecurity Strategy. Accordingly, ICAO developed the CyAP. The first edition of the CyAP was published in November 2020, and the second edition in January 2022.

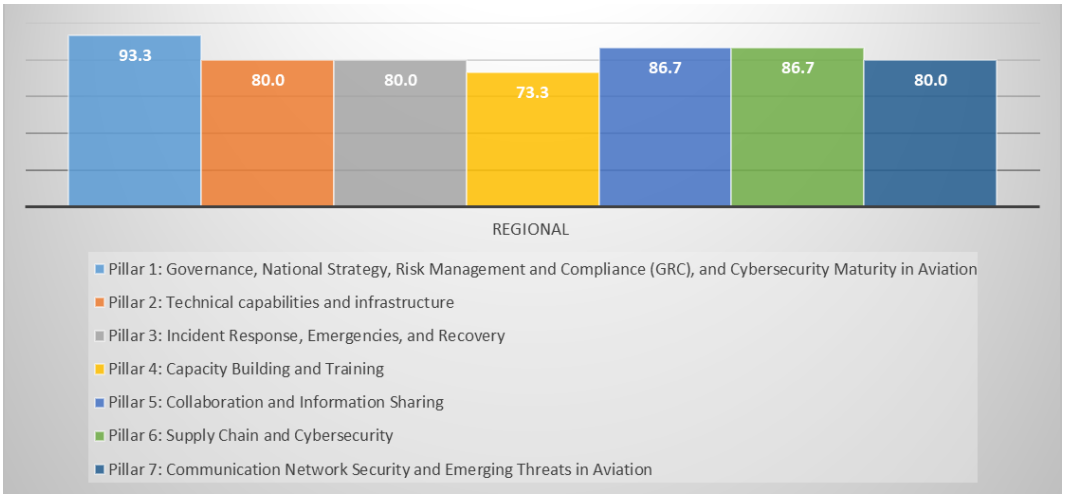
2. DISCUSSION

2.1 The CyAP provides the foundation for ICAO, States and stakeholders to work together, and proposes a series of principles, measures, and actions to achieve the objectives of the Aviation Cybersecurity Strategy's seven pillars. To that end, the CyAP develops the pillars of the Strategy into 32 Priority Actions, which are further broken down into 51 tasks to be implemented by ICAO, States, and stakeholders.

2.2 The meeting may wish to recall that the first meeting of the air navigation service Cybersecurity Working Group (ACS WG/1) conducted a gap analysis between CyAP and the implementation level in the MID Region. MIDANPIRG through Conclusion 20/43, endorsed the MID Region Action Plan and agreed that a follow-up survey should be developed.

2.3 The 4th meeting of the MID Regional Aviation Security and Facilitation Group (MID-RASFG/4, October, 2024) agreed that the ICAO-MID, in coordination with the RAFIT, develop a questionnaire and conduct a survey to follow-up the regional implementation of the recommendations of the Cybersecurity and Resilience Symposium. Consequently, the MID Office circulated the Questionnaire at **Appendix A.**

2.4 Five (5) States replied to the Questionnaire. The analysis of the questionnaire responses from five States highlights a concern regarding cybersecurity capacity-building programmes, particularly the limited availability of aviation-specific cybersecurity training and the effectiveness of current cybersecurity awareness initiatives.



2.5 The fifth meeting of the MID Regional Aviation Security and Facilitation Group (MID-RASFG/5, Doha, Qatar, 3 - 5 February 2026), through Conclusion 5/3, agreed that:

a) States that have not yet done so, send their replies to the questionnaire at Appendix A, to the MID Office, before 31 March 2026 to allow the RAFIT/9 meeting to review and analyse the results of the survey and propose the next course of actions;

b) States are urged to participate in global and regional cybersecurity events and follow-up on the development of the new Aviation Cybersecurity Manual; and

c) a Working Paper be presented by the Secretariat to the upcoming DGCA-MID/8 meeting proposing the establishment of a Regional multi-disciplinary Aviation Cybersecurity Task Force.

2.6 The CNS SG/15 meeting supported the MID-RASFG/5 Conclusion on the establishment of a regional multidisciplinary Aviation Cybersecurity Task Force. To avoid duplication of efforts and to optimize the use of States' resources, the meeting agreed to dissolve the ANS Cybersecurity Working Group (ACS WG) and agreed to the following Draft Decision:

DRAFT DECISION 15/13: DISSOLUTION OF ACS WG

That, in order to address Cybersecurity and Resilience through a multidisciplinary approach, ANS Cybersecurity Working group (ACS WG) is dissolved.

2.7 Concerning Cybersecurity capacity-building, the CNS SG/15 meeting recalled MIDANPIRG Conclusion 20/44 and noted that a Cybersecurity Event is planned for 2027, encouraging States to participate actively in this event.

2.8 The CNS SG/15 meeting recalled that the UAE developed and currently hosts the ATM Data Cybersecurity Portal (ADCS Portal). Through Conclusion 20/45, MIDANPIRG/20 encouraged States to make effective use of the Portal and to share their cybersecurity-related experiences. The CNS SG/15 meeting noted, however, that the Portal that designed to support the exchange of cybersecurity experiences and best practices, has not yet been used by States. It further noted that concerns about data confidentiality may be discouraging participation. The meeting also emphasized that ANS cybersecurity requires specialized skills and competencies that differ from those of traditional IT cybersecurity. The issue should be discussed in greater detail at the CNS SG/16 meeting.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the analysis of the Cybersecurity action plan implementation questionnaire;

b) urge States to participate actively in the planned Cybersecurity and resilience activity in 2027;

c) support the MID-RASFG/5 Conclusion in establishing a regional multi-disciplinary Aviation Cybersecurity Task Force; and

d) dissolve the ACS WG and endorse the Draft Decision 15/13.

استبيان - مخرجات ندوة الأمن السيبراني والمرونة- الدوحة 2023م

Cybersecurity Symposium Follow-up Survey - Doha 2023

1: Governance, National Strategy, Risk Management and Compliance (GRC), and Cybersecurity Maturity in Aviation	**المحور الأول: الحوكمة، الاستراتيجية الوطنية، إدارة المخاطر والامتثال(GRC) ، ونضج الأمن السيبراني للطيران**
Does the State have a national authority specialized in cybersecurity for the civil aviation sector ☐Yes ☐No	هل لدى الدولة هيئة وطنية متخصصة في الأمن السيبراني لقطاع الطيران المدني ☐نعم ☐لا
Has a clear legal framework for aviation cybersecurity been established ☐Yes ☐No	هل تم وضع إطار قانوني واضح للأمن السيبراني لقطاع الطيران المدني ☐نعم ☐لا
Does the State have a national cybersecurity strategy that includes the aviation sector ☐Yes ☐No	هل لدى الدولة استراتيجية وطنية للأمن السيبراني تشمل قطاع الطيران ☐نعم ☐لا
If a national strategy exists, to what extent does it cover the following aspects Rate from 1 to 5, where 1 = Not covered and 5 = Fully covered Protection against cyber threats Development of a secure aviation infrastructure …… Training and capacity building for personnel…… Risk management and emergency response…… International cooperation and information sharing……. Compliance with international cybersecurity standards in aviation…….	في حال وجود استراتيجية وطنية، ما مدى شمولها للجوانب التالية قيّم من 1 إلى 5، حيث 1 = غير مشمول و5 = مشمول بالكامل الحماية من التهديدات السيبرانية ..... تطوير بنية تحتية آمنة لقطاع الطيران..... تدريب وتأهيل الكوادر البشرية..... إدارة المخاطر والاستجابة للطوارئ..... التعاون الدولي وتبادل المعلومات..... الامتثال للمعايير الدولية للأمن السيبراني في الطيران.....
How is the effectiveness of the aviation cybersecurity strategy measured ☐Through regular audits ☐Through compliance assessments ☐Through incident analysis ☐There is no clear measurement	كيف يتم قياس مدى نجاح استراتيجية الأمن السيبراني للطيران في الدولة ☐عن طريق التدقيق بشكل دوري ☐عبر تقييمات الامتثال ☐من خلال تحليل الحوادث السابقة ☐لا يوجد قياس واضح
Are laws and policies regularly reviewed and updated to address evolving cyber threats ☐Yes ☐No	هل يتم مراجعة وتحديث التشريعات والسياسات الأمنية بشكل دوري لمواكبة التهديدات السيبرانية المتجددة ☐نعم ☐لا

Does the State have a specific governance, risk management, and compliance (GRC) framework for aviation cybersecurity ☐Yes ☐No	هل لدى الدولة إطار لحوكمة الأمن السيبراني وإدارة المخاطر والامتثال (GRC)خاص بقطاع الطيران ☐نعم ☐لا
What components are covered by the GRC framework for aviation cybersecurity (Select all that apply) ☐Cyber risk assessments and their impact on aviation operations ☐Development of security policies aligned with international standards ☐Compliance mechanisms with local and international regulations ☐Internal audits to monitor aviation cybersecurity compliance ☐Performance evaluation and continuous improvement mechanisms	ما المكونات التي يغطيها إطار GRC للأمن السيبراني للطيران (اختر ما ينطبق) ☐تقييم المخاطر السيبرانية وتأثيرها على العمليات الجوية ☐تطوير سياسات أمنية متوافقة مع المعايير الدولية ☐آليات الامتثال للتشريعات المحلية والدولية ☐تدقيق داخلي دوري لمراجعة الالتزام بأمن الطيران ☐آليات تقييم وتحسين مستمر للأداء السيبراني
Is there a clear mechanism to monitor compliance with aviation cybersecurity requirements ☐Yes ☐No	هل توجد آلية واضحة لمتابعة الامتثال لمتطلبات الأمن السيبراني في قطاع الطيران ☐نعم ☐لا
How effective is the cooperation between cybersecurity authorities and aviation regulatory bodies in ensuring compliance ☐No cooperation ☐Limited cooperation ☐Partial or ad-hoc cooperation when needed ☐Good and regular cooperation in some areas ☐Effective and integrated cooperation in all relevant areas	ما مدى فعالية التعاون بين الجهات المعنية بالأمن السيبراني والجهات التنظيمية لضمان الامتثال؟ ☐لا يوجد تعاون ☐ تعاون محدود ☐تعاون متوسط ويتم بشكل جزئي أو عند الحاجة فقط ☐تعاون جيد ومنتظم في بعض الجوانب ☐ تعاون فعّال ومتكامل في جميع الجوانب ذات العلاقة
What is the level of cybersecurity maturity in the civil aviation sector ☐Not mature – No clear cybersecurity policies or practices ☐Weak – Limited and uncoordinated initiatives exist ☐Moderate – Policies exist with some practices ☐Good – Policies are applied with continuous improvement ☐Fully mature – Comprehensive and systematic management based on best practices	ما مستوى نضج الأمن السيبراني في قطاع الطيران المدني؟ ☐غير ناضج – لا توجد سياسات أو ممارسات واضحة للأمن السيبراني ☐ضعيف – توجد مبادرات محدودة وغير مترابطة ☐متوسط – توجد سياسات وبعض الممارسات ☐جيد – يتم تطبيق السياسات مع وجود تحسينات مستمرة ☐ناضج تمامًا – توجد إدارة شاملة ومنهجية وفق أفضل الممارسات
Which standards or frameworks are used by the State to assess cybersecurity maturity in aviation	ما الأطر أو المعايير التي تستخدمها الدولة لتقييم نضج الأمن السيبراني في الطيران

☐ISO 27001 / 27005 ☐NIST Cybersecurity Framework ☐ICAO Aviation Cybersecurity Strategy ☐Other (please specify) ……	☐معيار ISO 27001 / 27005 ☐إطار الأمن السيبرانيNIST ☐استراتيجية الإيكاو للأمن السيبراني في الطيران ☐أخرى (يرجى التوضيح):----------
To what extent does the State comply with ICAO cybersecurity recommendations for the aviation sector ☐No compliance ☐Limited and irregular compliance ☐Partial compliance with some recommendations ☐Good compliance with regular follow-up ☐Full and systematic compliance in line with ICAO requirements	ما مدى التزام الدولة بتنفيذ توصيات منظمة الإيكاو (ICAO) المتعلقة بالأمن السيبراني في قطاع الطيران؟ ☐لا يوجد التزام ☐التزام محدود وغير منتظم ☐التزام جزئي ببعض التوصيات ☐التزام جيد مع وجود متابعة دورية ☐التزام كامل ومنهجي وفق متطلبات الإيكاو
Does the State have a documented national cybersecurity policy for the aviation sector ☐Yes ☐No	هل تمتلك الدولة سياسة وطنية موثقة للأمن السيبراني في قطاع الطيران ☐نعم ☐لا
What are the main challenges facing the State in developing or implementing aviation cybersecurity legislation ☐Lack of coordination among relevant entities ☐Shortage of specialized human resources ☐Absence of a unified international legal framework ☐Technical challenges related to infrastructure ☐Low compliance with international standards ☐Other (please specify)	ما أبرز التحديات التي تواجه الدولة في تطوير أو تنفيذ التشريعات الخاصة بالأمن السيبراني في قطاع الطيران ☐نقص التنسيق بين الجهات المعنية ☐نقص الموارد البشرية المتخصصة ☐غياب إطار قانوني دولي موحد ☐تحديات تقنية في البنية التحتية ☐ضعف الامتثال للمعايير الدولية ☒أخرى (يرجى التوضيح):----------
	المحور الثاني: القدرات التقنية والبنية التحتية
Does the State have a Security Operations Center (SOC) to monitor cybersecurity activities related to civil aviation ☐Yes ☐No ☐Under development	هل تمتلك الدولة مركز عمليات أمنية لمراقبة الأنشطة السيبرانية المرتبطة بالطيران المدني؟ ☐نعم ☐لا ☐قيد الانشاء
What is the readiness level of Security Operations Centers (SOC) to handle advanced cyber threats ☐Not ready	ما مدى جاهزية مراكز العمليات الأمنية (SOC) للتعامل مع التهديدات السيبرانية المعقدة؟ ☐غير جاهزة
☐Low readiness	*لا توجد قدرات كافية لرصد أو الاستجابة للتهديدات المعقدة.*

	☐جاهزية منخفضة
☐Moderate readiness	*القدرات الأساسية متوفرة، ولكن هناك نقص في الأدوات أو المهارات أو الإجراءات الفعّالة.* ☐جاهزية متوسطة
☐Good readiness	*يوجد مستوى مقبول من الرصد والاستجابة، لكن لا تزال هناك فجوات في مواجهة التهديدات المتقدمة.* ☐جاهزية جيدة
	المركز يمتلك تقنيات وكفاءات جيدة، ويستطيع التعامل مع التهديدات المعقدة. ☐جاهزة تماماً
Are penetration tests conducted regularly on civil aviation systems ☐Yes ☐No ☐Sometimes	*المركز يعمل بكفاءة عالية، ويطبق أفضل الممارسات، وقادر على التصدي بفعالية لكافة أنواع التهديدات السيبرانية المعقدة.* هل يتم إجراء اختبارات اختراق بشكل منتظم على أنظمة الطيران المدني؟ ☐نعم ☐لا ☐احياناً
What types of tools and technologies are used to detect and analyze cyber threats (Select all that apply) ☐Intrusion Detection and Prevention Systems (IDS/IPS) ☐Cybersecurity Operations Centers (SOC) ☐Threat Intelligence Platforms ☐Log Analysis Tools ☐Other (please specify) ……..	ما أنواع الأدوات والتقنيات المستخدمة لرصد وتحليل التهديدات السيبرانية؟ (اختر ما ينطبق) ☐أنظمة كشف التسلل والوقاية(IDS/IPS) ☐مراكز عمليات الأمن السيبراني(SOC) ☐منصات تبادل معلومات التهديدات (Threat Intelligence Platforms) ☐تحليلات السجلات(Log Analysis Tools) ☐أخرى (يرجى التوضيح):----------
Are cyber incidents documented and analyzed, and are reports shared with relevant entities ☐Yes ☐No	هل يتم توثيق وتحليل الحوادث السيبرانية، ومشاركة التقارير مع الجهات المعنية؟ ☐نعم ☐لا

Is Identity and Access Management (IAM) implemented in civil aviation systems ☐Yes ☐No ☐In progress	هل يتم تطبيق ضوابط إدارة الهوية والوصول IAM في أنظمة الطيران المدني؟ ☐نعم ☐لا ☐قيد التطبيق
Is Multi-Factor Authentication (MFA) used to access sensitive systems ☐Yes ☐No	هل يتم استخدام المصادقة متعددة العوامل (MFA) للوصول إلى الأنظمة الحساسة؟ ☐نعم ☐لا
What is the maturity level of the current technical infrastructure in supporting aviation cybersecurity requirements ☐Very weak ☐Weak ☐Moderate ☐Good ☐Excellent	ما مدى نضج البنية التحتية التقنية الحالية في دعم متطلبات الأمن السيبراني للطيران؟ ☐ضعيفة جداً ☐ضعيفة ☐متوسطة ☐جيدة ☐ممتازة
What are the main cybersecurity challenges faced in enhancing aviation cybersecurity (You may select more than one) ☐Lack of qualified technical personnel ☐Insufficient funding and financial support for cybersecurity ☐Outdated systems and technologies ☐Lack of integration between existing cybersecurity tools and systems ☐Low cybersecurity awareness among employees ☐Absence of clear cybersecurity policies and procedures ☐Other (please specify) …….	ما التحديات السيبرانية الرئيسية التي تواجهها في تعزيز الأمن السيبراني ؟ (يمكن اختيار اكثر من تحدي) ☐نقص الكفاءات الفنية المؤهلة ☐ضعف التمويل والدعم المالي المخصص للأمن السيبراني ☐تقادم الأنظمة والتقنيات المستخدمة ☐عدم تكامل الأدوات والأنظمة الأمنية المستخدمة حاليًا ☐ضعف الوعي السيبراني لدى الموظفين ☐غياب السياسات والإجراءات الواضحة للأمن السيبراني ☐أخرى (يرجى التوضيح) .....
Incident Response, Emergencies, and Recovery	**المحور الثالث: الاستجابة للحوادث والطوارئ والتعافي منها**

Does the State have a cyber incident response plan for the civil aviation sector ☐Yes ☐No ☐Under development	هل لدى الدولة خطة استجابة للحوادث السيبرانية لمنظومة الطيران المدني؟ ☐نعم ☐لا ☐قيد التطوير
Is there a disaster recovery plan specifically designed for civil aviation systems ☐Yes ☐No ☐Under development	هل توجد خطة تعافي من الكوارث السيبرانية (Disaster Recovery) مخصصة لأنظمة الطيران المدني؟ ☐نعم ☐لا ☐قيد التطوير
Are regular exercises and drills conducted to simulate responses to cyber incidents in civil aviation ☐Yes – conducted regularly ☐Yes – but not regularly ☐No – no exercises or drills are conducted	هل يتم تنفيذ تدريبات وتمارين دورية لمحاكاة الاستجابة لحوادث سيبرانية في الطيران المدني؟ ☐نعم – بشكل دوري ومنتظم ☐نعم – ولكن بشكل غير منتظم ☐لا – لا يتم تنفيذ تدريبات أو تمارين
What is the readiness level of cyber incident response teams in the civil aviation sector ☐Not ready ☐Weak ☐Moderate ☐Good ☐Fully ready to handle various incidents	ما مدى جاهزية فرق الاستجابة للحوادث السيبرانية في الطيران المدني؟ ☐غير جاهزة ☐ضعيفة ☐متوسطة ☐جيدة ☐جاهزة تمامًا للتعامل مع مختلف الحوادث
Have lessons learned from previous cyber incidents in the aviation sector been documented ☐Yes ☐No	هل تم توثيق الدروس المستفادة من الحوادث السيبرانية السابقة في قطاع الطيران المدني؟ ☐نعم ☐لا
Is there a clear timeline for recovery from cyber incidents related to civil aviation ☐Yes ☐No	هل هناك إطار زمني واضح للتعافي من الحوادث السيبرانية المرتبطة بالطيران المدني؟ ☐نعم ☐لا

What are the key challenges facing the State in enhancing its readiness to respond to cyber incidents in civil aviation (Select all that apply) ☐Lack of specialized personnel in aviation cyber incident response ☐Insufficient cyber drills and exercises ☐Weak coordination between relevant entities ☐Lack of a unified platform for sharing threat and incident information ☐Low cybersecurity awareness among aviation staff ☐Other (please specify)	ما أبرز التحديات التي تواجه الدولة في تعزيز جاهزيتها للاستجابة للحوادث السيبرانية في قطاع الطيران المدني؟ *(أختر ما ينطبق)* ☐نقص الكوادر المتخصصة في مجالات الاستجابة السيبرانية للطيران المدني. ☐عدم كفاية التدريبات والتمارين السيبرانية. ☐ضعف التنسيق بين الجهات. ☐عدم توفر منصة موحدة لمشاركة المعلومات حول التهديدات والحوادث. ☐ضعف الوعي السيبراني لدى العاملين في القطاع. ☐أخرى (يرجى التوضيح): .....
Pillar 4: Capacity Building and Training	**المحور الرابع: بناء القدرات والتدريب**
Does the State have a national plan for qualifying and training personnel working in cybersecurity for the civil aviation sector? ☐Yes ☐No ☐Under development	هل تمتلك الدولة خطة وطنية لتأهيل وتدريب الكوادر العاملة في الأمن السيبراني لقطاع الطيران المدني؟ ☐نعم ☐لا ☐قيد التطوير
Which groups or categories are targeted by training and qualification plans in the field of cybersecurity for the civil aviation sector (Select all that apply) ☐All civil aviation personnel Technicians and specialists in air navigation and ☐aviation systems ☐Personnel working on critical or sensitive systems ☐IT and infrastructure or network specialists ☐Cybersecurity professionals ☐Leadership and supervisory positions ☐OTHER……..	ما الجهات أو الفئات المستهدفة ضمن خطط التدريب والتأهيل في مجال الأمن السيبراني لقطاع الطيران المدني؟ *(اختر ما ينطبق).* ☐جميع منسوبي الطيران المدني ☐الفنيين والمختصين في أنظمة الملاحة الجوية وأنظمة الطيران. ☐العاملين على الأنظمة الحرجة أو الحساسة. ☐التقنيين والمختصين بالبنية التحية التقنية والشبكات. ☐المختصين بالأمن السيبراني. ☐القيادات والوظائف الاشرافية. ☐أخرى (يرجى التوضيح).....
What types of cybersecurity training programs are currently available for the civil aviation sector (Select all that apply)	ما نوع البرامج التدريبية المتوفرة حاليًا في مجال الأمن السيبراني لقطاع الطيران المدني؟

☐Internal training courses ☐International training programs ☐No current training programs	*(اختر ما ينطبق)* ☐دورات تدريبية داخلية ☐برامج تدريبية عالمية ☐لا توجد برامج تدريبية حالية
Are there continuous annual training plans ☐Yes ☐No	هل توجد خطط تدريب مستمرة سنويًا؟ ☐نعم ☐لا
Is the effectiveness of training programs evaluated ☐Yes through participant surveys and feedback ☐Yes through testing and performance evaluation ☐No evaluation is conducted	هل يتم تقييم فعالية البرامج التدريبية؟ ☐نعم، عبر استبيانات وآراء المشاركين ☐نعم، عبر اختبارات وتقييم أداء ☐لا يتم التقييم
How effective is the training in improving cybersecurity awareness among civil aviation staff ☐Very Poor ☐Poor ☐Moderate ☐Good ☐Excellent	ما مدى فعالية التدريب في تحسين مستوى الوعي السيبراني بين العاملين في الطيران المدني؟ ضعيف جدًا ضعيف متوسط جيد ممتاز
Are there awareness campaigns or periodic bulletins about cybersecurity in aviation ☐Yes regularly ☐Yes but irregularly ☐No campaigns exist	هل توجد حملات توعوية أو نشرات دورية حول الأمن السيبراني في الطيران؟ ☐نعم بانتظام ☐نعم لكن غير منتظم ☐لا توجد
Is cybersecurity included in the basic orientation programs for new employees ☐Yes ☐No	هل يتم تضمين الأمن السيبراني ضمن برامج التأهيل الأساسية للعاملين الجدد؟ ☐ نعم ☐لا
Is there a dedicated budget for cybersecurity training in the aviation sector ☐Yes ☐No	هل يتم تخصيص ميزانية واضحة لتدريب الأمن السيبراني في قطاع الطيران؟ ☐ نعم ☐لا
What are the key challenges facing the State in building cybersecurity capabilities for the aviation	ما أبرز التحديات التي تواجه الدولة في بناء القدرات السيبرانية لقطاع الطيران؟ (اختر ما ينطبق)

sector (Select all that apply) ☐Lack of qualified trainers ☐Limited resources ☐Lack of institutional interest in cybersecurity Weak coordination between training and regulatory ☐bodies Other…… ☐……..	☐نقص المدربين المؤهلين ☐ضعف الموارد ☐عدم الاهتمام المؤسسي بالأمن السيبراني ☐ضعف التنسيق بين الجهات التدريبية والتنظيمية ☐أخرى.....
Pillar 5: Collaboration and Information Sharing	**المحور الخامس: التعاون ومشاركة المعلومات**
Does the State have formal mechanisms for cybersecurity information sharing among entities concerned with the civil aviation sector ☐Yes ☐No ☐Under development	هل لدى الدولة آليات رسمية لتبادل المعلومات السيبرانية بين الجهات المعنية بقطاع الطيران المدني؟ ☐نعم ☐لا ☐قيد التطوير
What types of information are shared among entities in the field of aviation cybersecurity ☐Discovered security vulnerabilities ☐Indicators of Compromise (IOCs) ☐Previous incidents and lessons learned ☐Security practices and guidelines ☐No current information sharing	ما نوع المعلومات التي يتم تبادلها بين الجهات في مجال الأمن السيبراني للطيران؟ ☐الثغرات الأمنية المكتشفة ☐مؤشرات الاختراق(IOCs) ☐حوادث سابقة ودروس مستفادة ☐ممارسات وإرشادات الحماية ☐لا يوجد تبادل للمعلومات حاليًا
Is there a national entity responsible for coordinating cybersecurity information sharing ☐Yes ☐No	هل توجد جهة وطنية مسؤولة عن تنسيق تبادل المعلومات السيبرانية؟ ☐نعم ☐لا
How effective are the cybersecurity information-sharing channels between government entities and the aviation sector ☐Very weak ☐Weak ☐Moderate ☐Good ☐Very effective	ما مدى فعالية قنوات تبادل المعلومات السيبرانية بين الجهات الحكومية وقطاع الطيران؟ ☐ضعيفة جدًا ☐ضعيفة ☐متوسطة ☐جيدة ☐فعالة

Which platforms or mechanisms does the State use to share cybersecurity information ☐CERT ☐Other (please specify)……..	ما المنصات أو الآليات التي تستخدمها الدولة لتبادل المعلومات السيبرانية؟ (اختر ما ينطبق) ☐CERT ☐أخرى.....
Are there obstacles that limit the sharing of cybersecurity information with other parties ☐Sensitivity of information and lack of clear information-sharing policy ☐Absence of formal exchange channels ☐Lack of an information-sharing culture ☐Other (please specify)……..	هل توجد معوقات تحدّ من مشاركة المعلومات السيبرانية مع الأطراف الأخرى؟ (اختر ما ينطبق) ☐حساسية المعلومات وعدم وضوح سياسة مشاركة المعلومات ☐غياب القنوات الرسمية للتبادل ☐عدم وجود ثقافة مشاركة المعلومات ☐أخرى.....
Is information related to cyber incidents or threats shared in a timely manner with relevant entities ☐Always ☐Sometimes ☐Rarely ☐Not shared	هل يتم مشاركة المعلومات المتعلقة بالحوادث أو التهديدات السيبرانية في وقت مناسب مع الجهات ذات العلاقة؟ ☐دائمًا ☐أحيانًا ☐نادرًا ☐لا تتم المشاركة
To what extent does the State need support or enhancement in establishing cybersecurity information-sharing mechanisms for the aviation sector ☐Very high ☐High ☐Moderate ☐Low ☐No current need	ما مدى حاجة الدولة إلى دعم أو تعزيز في مجال بناء آليات مشاركة المعلومات السيبرانية لقطاع الطيران؟ ☐عالية جدًا ☐عالية ☐متوسطة ☐منخفضة ☐لا توجد حاجة حالية
Pillar 6: Supply Chain and Cybersecurity	**المحور السادس: سلاسل التوريد والأمن السيبراني**
Does the State have a framework for assessing cybersecurity risks related to the aviation sector's supply chains ☐Yes ☐No ☐Under development	هل لدى الدولة إطار لتقييم المخاطر السيبرانية المرتبطة بسلاسل التوريد في قطاع الطيران؟ ☐نعم ☐لا ☐قيد التطوير
Are cybersecurity requirements included in maintenance and operations contracts or supplier agreements in the aviation sector ☐Yes, always	هل يتم تضمين متطلبات الأمن السيبراني ضمن عقود الصيانة والتشغيل أو التعاقد مع الموردين في قطاع الطيران؟ ☐نعم بشكل دائم

☐Yes, in some cases ☐No	☐نعم في بعض الحالات ☐لا
Is there a list of security standards or policies that suppliers are required to comply with Yes☐ No☐ ☐ Under preparation	هل توجد قائمة معايير أو سياسات أمنية يجب على الموردين الالتزام بها؟ ☐نعم ☐لا ☐تحت الإعداد
Is the compliance of suppliers with cybersecurity requirements assessed regularly ☐Yes ☐No ☐Sometimes	هل يتم تقييم التزام الموردين بمتطلبات الأمن السيبراني بشكل دوري؟ ☐نعم ☐لا ☐أحيانًا
Are cybersecurity audits or inspections conducted on contracted suppliers ☐Yes ☐No	هل يتم تنفيذ عمليات تدقيق أو تفتيش أمني على الموردين المتعاقدين؟ ☐نعم ☐لا
What is the maturity level of the State or organization in applying cybersecurity practices to suppliers ☐Very low ☐Low ☐Moderate ☐Good ☐Excellent	ما مستوى نضج الدولة أو الجهة في تطبيق ممارسات الأمن السيبراني على الموردين؟ ☐ضعيف جدًا ☐ضعيف ☐متوسط ☐جيد ☐ممتاز
What challenges do you face in securing the cybersecurity of supply chains in the aviation sector (Select all that apply) ☐Lack of clear legislation or policies ☐Low cybersecurity awareness among suppliers ☐Limited resources for assessment and review ☐Complexity and number of involved parties ☐Other (please specify)	ما التحديات التي تواجهكم في تأمين سلاسل التوريد السيبرانية في قطاع الطيران؟ (اختر ما ينطبق) ☐نقص التشريعات أو السياسات الواضحة ☐ضعف الوعي السيبراني لدى الموردين ☐قلة الموارد المخصصة للتقييم والمراجعة ☐تعقيد السلاسل وكثرة الأطراف ☐أخرى.....
Do you consider supply chains a primary cybersecurity threat source in the aviation sector ☐Yes ☐No	هل ترون أن سلاسل التوريد تمثل مصدر تهديد رئيسي للأمن السيبراني في قطاع الطيران؟ ☐نعم ☐لا

☐Sometimes	☐إلى حد ما
Pillar 7: Communication Network Security and Emerging Threats in Aviation	**المحور السابع: أمن شبكات الاتصالات والتهديدات الناشئة في الطيران**
Is there a policy in place to secure communication networks within the aviation sector ☐Yes ☐No ☐Under development	هل توجد سياسة لتأمين شبكات الاتصالات الخاصة بقطاع الطيران؟ ☐نعم ☐لا ☐قيد التطوير
What types of networks are included in aviation cybersecurity plans (Select all that apply) ☐Airport operations and critical systems networks ☐Air navigation and aircraft communication networks Security networks (e.g., surveillance and access control ☐systems) ☐Internal administrative and service networks ☐ Other (please specify)	ما أنواع الشبكات التي تُشمل ضمن خطط الأمن السيبراني في قطاع الطيران؟ (اختر ما ينطبق) ☐شبكات تشغيل المطار والأنظمة التشغيلية الحيوية ☐شبكات الملاحة الجوية والربط مع الطائرات ☐الشبكات الأمنية (مثل أنظمة المراقبة والتحكم في الدخول) ☐الشبكات الإدارية والخدمية الداخلية ☐أخرى.....
Are encryption technologies used to protect data exchanged through communication systems ☐Yes ☐No	هل يتم استخدام تقنيات تشفير لحماية البيانات المتبادلة ضمن أنظمة الاتصالات؟ ☐نعم ☐لا
Is there a periodic risk assessment for communication systems used in civil aviation ☐ Yes ☐No ☐Sometimes	هل هناك تقييم دوري لمخاطر أنظمة الاتصالات المستخدمة في الطيران المدني؟ ☐نعم ☐لا ☐أحيانًا
What are the main challenges facing the State in securing communication networks in the aviation sector (Select all that apply) ☐Outdated infrastructure ☐Shortage of qualified cybersecurity communication specialists ☐Lack of updated and specialized standards ☐Other (please specify)……..	ما أبرز التحديات التي تواجه الدولة في تأمين شبكات الاتصالات المرتبطة بالطيران المدني؟ (اختر ما ينطبق) ☐تقادم البنى التحتية ☐قلة الكوادر المؤهلة في الاتصالات السيبرانية ☐عدم وجود معايير محدثة ومتخصصة ☐أخرى.....

- END -