



International Civil Aviation Organization

**MIDANPIRG Communication, Navigation and Surveillance Sub-Group
(CNS SG/15)**

(Doha, Qatar, 11 – 14 May 2026)

Agenda Item 6: Air Navigation Services Cyber Résilience

AIR NAVIGATION SERVICES CYBER RESILIENCE

(Presented by Secretariat)

SUMMARY

This paper presents the actions undertaken by the Regional Aviation Security Groups in relation to Cybersecurity, including the implementation of the action plan questionnaire and the invitation to a meeting to discuss ways to activate and enhance the use of ATM data cybersecurity portal (ADCS).

Action by the meeting is at paragraph 3.

REFERENCES

- MIDANPIRG/20 Report
- ICAO MID RAFIT/5 Report (3 - 5 February 2026, Doha, Qatar)

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.

2. DISCUSSION

ICAO Cybersecurity Survey

2.1 The meeting may wish to recall that the first meeting of the ANC cybersecurity working group (ACS WG/1) conducted gap analysis between ICAO Cybersecurity Action plan and the current implementation level in the MID region. The action plan was endorsed by MIDANPIRG, through the following Conclusion:

MIDANPIRG CONCLUSION 20/43: MID REGION ANS CYBERSECURITY ACTION PLAN

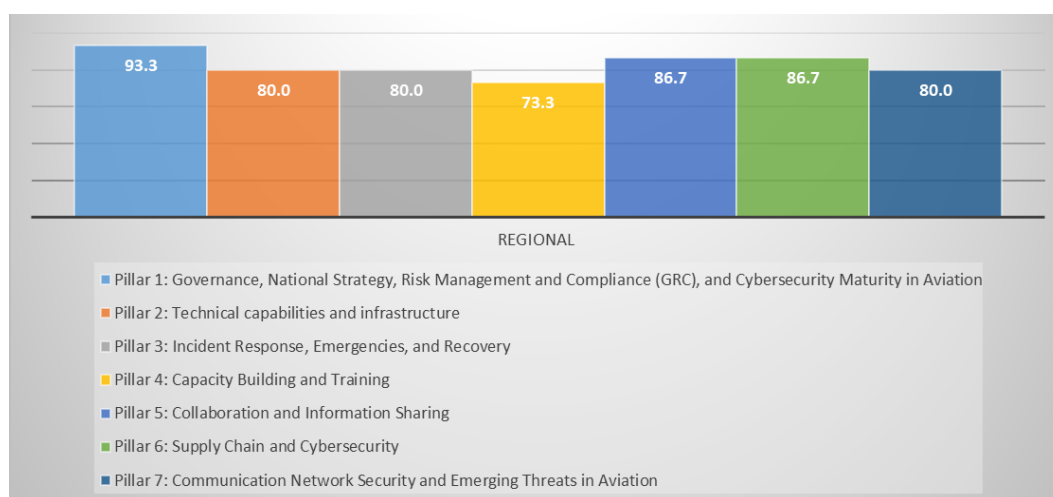
That, in order to assist States achieving the objectives of ICAO Cyber Security Strategy seven pillars in ANS area in the MID Region:

- a) *the MID Region ANS Cybersecurity actions plan at Appendix 6.6G is endorsed;*
- b) *urge States to implement identified actions in a timely manner; and*
- c) *ACS WG to develop a survey to establish how States have implemented the identified actions.*

2.2 The fifth meeting of Regional Aviation Security and Facilitation Group (MID-RASFG/5, Doha, Qatar, 3 - 5 February 2026) agreed that ICAO-MID in coordination with the Regional Aviation Security and Facilitation Implementation Team (RAFIT) to:

- 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.

2.3 The MID Office circulated the Questionnaire at ***Appendix A***. Only five (5) States out of fifteen (15) replied to the Questionnaire.



ICAO Cybersecurity Capacity Building Activities

2.4 MIDAPIRG/20 meeting requested ICAO, through Conclusion 20/44, to organize capacity building activities on ANS Cybersecurity in 2024-2025.

2.5 The meeting may wish to recall that an ANS Cyber Resilience Tabletop Exercise (TTX) was successfully conducted 13-15 November 2022, in order to identify gaps in incidents response, business continuity and decision-making process during a cyber-attack incident.

2.6 The analysis of the questionnaire in (2.3) demonstrates common concern on cybersecurity capacity building programme highlighting the lack of aviation related cybersecurity specialized training and the effectiveness of current cybersecurity awareness.

2.7 With the capacity building deficiency as the major concern and the insufficient cybersecurity expertise, industry's ability to respond to evolving threats diminish. To elevate the level of cybersecurity awareness and tools provided by ICAO and industry's best practices, States are urged to participate in global and regional cybersecurity events and follow-up on the development of the new Aviation Cybersecurity Manual and capacity building activities.

2.8 The meeting may wish to note that ICAO plan to conduct a regional capacity building activity on Cybersecurity and resilience in 2027.

ATM DATA Cybersecurity Data Portal (ADCS)

2.9 In accordance with the MID Region ANS Cyber Security action plan, States should share experience on cyber threats and incidents. In this regard, the meeting may wish to recall that UAE developed and hosted ATM data cybersecurity portal (ADCS Portal). MIDANPIRG20/45 urged States, through Conclusion 20/45, to use the ADCS effectively, share their experience related to cybersecurity, through the ADCS Portal.

2.10 It has been observed that the ADCS portal, established for sharing cybersecurity-related experiences and best practices, has not yet been utilized by the states. To better understand the status and encourage broader participation, the meeting may wish to discuss the challenges, and constraints affecting the use of the portal. The discussion may also cover the process the measures required to promote its effective adoption, regular usage, and active contribution by all states.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

- a) note the analysis of the Cybersecurity action plan implementation questionnaire;
- b) discuss the challenges, and constraints affecting the use of the ADCS portal including the measures required to promote its effective adoption, regular usage, and active contribution by all States;
- c) urge States to participate actively in the planned Cybersecurity and resilience activity in 2027; and
- d) support the RAFIT/5 Conclusion in establishing a regional multi-disciplinary Aviation Cybersecurity Task Force, to dissolve the ACS WG and agree on the following Draft Decision:

DRAFT DECISION 15/X: DISSOLUTION OF ACS WG

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

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

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

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

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

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

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

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

<input type="checkbox"/> Internal training courses <input type="checkbox"/> International training programs <input type="checkbox"/> No current training programs	(اختر ما ينطبق) <input type="checkbox"/> دورات تدريبية داخلية <input type="checkbox"/> برامج تدريبية عالمية <input type="checkbox"/> لا توجد برامج تدريبية حالية
Are there continuous annual training plans <input type="checkbox"/> Yes <input type="checkbox"/> No	هل توجد خطط تدريب مستمرة سنويًا؟ <input type="checkbox"/> نعم <input type="checkbox"/> لا
Is the effectiveness of training programs evaluated <input type="checkbox"/> Yes through participant surveys and feedback <input type="checkbox"/> Yes through testing and performance evaluation <input type="checkbox"/> No evaluation is conducted	هل يتم تقييم فعالية البرامج التدريبية؟ <input type="checkbox"/> نعم، عبر استبيانات وآراء المشاركين <input type="checkbox"/> نعم، عبر اختبارات وتقييم أداء <input type="checkbox"/> لا يتم التقييم
How effective is the training in improving cybersecurity awareness among civil aviation staff <input type="checkbox"/> Very Poor <input type="checkbox"/> Poor <input type="checkbox"/> Moderate <input type="checkbox"/> Good <input type="checkbox"/> 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 <input type="checkbox"/> Yes regularly <input type="checkbox"/> Yes but irregularly <input type="checkbox"/> No campaigns exist	هل توجد حملات توعوية أو نشرات دورية حول الأمن السيبراني في الطيران؟ <input type="checkbox"/> نعم بانتظام <input type="checkbox"/> نعم لكن غير منتظم <input type="checkbox"/> لا توجد
Is cybersecurity included in the basic orientation programs for new employees <input type="checkbox"/> Yes <input type="checkbox"/> No	هل يتم تضمين الأمن السيبراني ضمن برامج التأهيل الأساسية للعاملين الجدد؟ <input type="checkbox"/> نعم <input type="checkbox"/> لا
Is there a dedicated budget for cybersecurity training in the aviation sector <input type="checkbox"/> Yes <input type="checkbox"/> No	هل يتم تخصيص ميزانية واضحة لتدريب الأمن السيبراني في قطاع الطيران؟ <input type="checkbox"/> نعم <input type="checkbox"/> 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)

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

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

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

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