网 络 安 保 行 动 计 划

由秘书长授权出版

2022 年 1 月，第二版

国际民用航空组织

术语和定义[1]

caISMS：民航信息安保管理体系

一种建立、实施、运营、监测、审查、维护和改进信息资产保护的模式，以实现民用航空目标；它基于风险评估和本组织的风险接受水平，旨在处理和管理风险。

来源 ISO27000:2009

网络安保

旨在确保系统、网络、程式、设备、信息和数据免受攻击、损坏、未经授权的访问、使用和/或利用的机密性、完整性、可用性和整体保护的技术、控制和措施以及流程和实践的主体。

网络安保政策

网络安保政策记录了一个组织管理网络安保威胁的意图和方向，由最高管理层所表述。它是组织内的一份书面文件，概述如何保护组织免受网络安保威胁，以及在发生网络安保威胁时如何处理这些事故征候和事件。

事件

在系统、服务或网络状态中查出发生的事件，表明其可能违反信息安保政策或控制失败，或是一种先前未知的可能与安保有关的情况[ISO/IEC 27035]。应注意的是，“发生”需要从广义上加以考虑，而不应理解为仅涵盖航空安全情景下发生具有或可能具有重要意义之(安全)事件的术语。

事故征候

一个或一系列不想要的或意外的信息安保事件，这些事件很可能破坏业务运营并威胁信息安保[ISO/IEC 27035-1]

信息安保

保护信息的机密性、完整性和可用性。此外还可涉及其他属性，如真实性、问责性、不可否认性和可靠性。[BS ISO/IEC 27000:2018]

信息共享

一个实体向一个或多个其他实体提供信息以促进作出基于风险的决策和促进最佳做法的过程。

风险矩阵

对风险的组成部分(威胁、可能性、影响/后果和薄弱性)、实施的风险缓解措施以及最终的剩余风险进行排名和显示的工具。

---

[1] 仍在审查。

威胁实体(或行为者)

对影响或可能影响一个组织或系统的事故征候负部分或全部责任的实体。

薄弱性

在信息系统、系统安保程序、内部控制或实施程序中可能被威胁实体利用或触发的弱点。这可以是直接或间接支持航空系统一项功能的系统。

执行摘要

国际民用航空组织大会第 39 届会议重申了保护民航重要基础设施系统和数据免受网络攻击并得到国际民航组织、其成员国和业界利害攸关方采取行动的全球承诺之重要性和紧迫性，以期以协作和系统方式处理民航网络安保问题，减缓相关威胁和风险。第 A39-19 号决议 — 解决民用航空网络安保问题确定了各国和其他利害攸关方在这方面应采取的行动。国际民航组织大会第三十九届会议还指示国际民航组织制定一项全面的网络安保工作计划。

为了满足大会的期望，秘书处网络安保研究小组（SSGC）制定了民航网络安保战略。

国际民航组织大会第 40 届会议通过了经修订的关于解决民用航空网络安保问题的 A40-10 号决议，其中呼吁各国执行网络安保战略，并强调必须为该战略制定一项可持续的实施计划，并继续努力制定一个强有力的网络安保框架。

网络安保行动计划（CyAP）为各国、业界、利害攸关方和国际民航组织合作奠定了基础，以发展用以识别、预防、发现、回击对民用航空的网络攻击并从中恢复的能力，并打造一个坚实的合作框架。制定该行动计划的目的是提出一系列原则、措施和行动，以实现该战略七大支柱的目标。

第 1 章

引言

1.1 背景

1.1.1 在当前民航环境下，空中交通都预测为将呈现长期增长，技术发展日新月异，运行变得更加复杂，运行环境也随之愈加具有挑战性。快速的技术变革正在改变民航的运营方式，使其系统更容易受到网络安保威胁。恶意的网络活动可以通过各种方式影响民航，从运营的轻微中断到发生灾难性的结果都包括在内。风险正在迅速增加，十分需要在国际、地区和国家各级建立一个可持续的网络安保框架。

1.1.2 建立健全的网络安保基础设施，有赖于各国、业界和国际民航组织之间的大力合作，从而树立共同的网络安保意识，最终实现更可靠、复原力更强的民航系统。

1.1.3 国际民航组织根据联合国安理会各项决议不断作出调整，以适应持续变化的全球威胁形势，这些决议申明各国有责任确保在其领土内运行的航空服务的安全，并呼吁所有国家与国际民航组织合作，确保按照《芝加哥公约》并根据当前风险对国际安保标准进行审查、更新和落实。随着对民航的网络安保威胁不断演变并可能日益普遍，根据联合国安理会第 2341(2017)号决议的规定，国际民航组织着重于建立适当的机制，以减缓和减少通过网络载体的非法干扰以及可能影响运行安全的事件对重要航空基础设施造成的风险。

1.1.4 在此方面，为了妥善实现航空网络安保战略七大支柱的目标并建立网络安保框架，制定了这一行动计划。

1.2 宗旨

1.2.1 该计划是一份活文件，将随着网络安保的发展而演变并将定期更新，以反映由于第 3 章和第 4 章所述的差距分析和活动等产生的所需变化。 网络安保行动计划描述了实施国际民航组织航空网络安保战略的目标和行动。本文件所列内容反映了不同地区/国家或业界已完成或正在进行的工作。它包括从网络安保的角度对航空系统目前搌现状攡较之于该战略提出的搌未来攡情况的分析结果，并制定一个可以推动这种演变的行动计划，以实现战略愿景。

1.2.2 鉴于为实施本文件所列各项目标和行动需要开展的大量工作，附录 A 提出了一种分阶段的做法，并确定短期、中期和长期目标。

1.3 风险背景

1.3.1 在民用航空中，网络安保并不是新概念。然而，随着网络安保威胁的日益普遍，网络安保已成为讨论和分析民航系统风险和薄弱性的核心内容之一。民航部门尤其面临风险，因该部门各个组成部分的职能和数字化相互依赖的程度与日俱增，使网络攻击更易得手，同时也因为民航部门目前使用的网络防御机制还不足以应对这种持续不断适应的威胁。

1.3.2 国际民航组织航空安保专家组最近对薄弱性进行具有恐怖主义性质的攻击所造成的风险水平评定为中等。这一评估基于网络安保领域的残余薄弱性，并假定各国已有效实施附件 17 —《安保》规定。然而，网络风险正在迅速演变，必须对所有可能影响到民航运行安保和安全这两方面的网络攻击者的形态进行评估。此外，网络攻击的来源往往难以追查，因此查找和起诉网络攻击往往十分复杂，难以实现，而同时使得攻击的受害者或其保险方承担恢复的代价。基于这些原因，国际民航组织、各国和业界必须携手行动，系统实施网络安保战略，这一点极为重要。

1.4 行动计划的益处

1.4.1 网络安保行动计划旨在确保国际民航组织、成员国和业界承诺实施航空网络安保战略并实现其七大支柱所述的目标。一个强大的网络安保框架将加强民航系统，并将有利于整个全球航空界。

第 2 章

目标

2.1 网络安保行动计划的目标

2.1.1 网络安保行动计划的目标是实现网络安保战略七个支柱所述目标，并建立一个强有力的民航网络安保框架。

2.1.2 构成当前行动计划基础的原则如下：

a) 成员国对《国际民用航空公约》（《芝加哥公约》）规定的确保民用航空运行的安全、安保和连续性的网络安保义务的理解；

b) 协调成员国当局之间的航空网络安保措施，确保对航空网络安保进行高效和有效的全球管理；和

c) 所有民航利害攸关方承诺进一步发展网络应变能力，保护航空免遭可能影响到航空运输系统安全、安保和连续性的网络攻击，无论这种攻击来自于何种威胁行动者形态。

2.2 适用

2.2.1 本文件主要面向国际民航组织成员国和业界，通过全面、协调和整体做法，作为协助它们管理民用航空网络安保风险的一种手段。

2.2.2 各国、业界和其他相关的利害攸关方应该采取本行动计划所提出的行动。

第 3 章

战略行动计划

3.1 航空网络安保战略的七大支柱

3.1.1 制定了本章所载的各项要素，旨在提出一系列原则、措施和行动，以实现航空网络安保战略七大支柱的目标，即：

1. 国际合作
2. 治理
3. 有效的立法和规章
4. 网络安保政策
5. 信息共享
6. 事故征候管理和应急规划
7. 能力建设、培训和网络安保文化

支柱 1 — 国际合作
• 在国内和国际层面所有利害攸关方之间开展合作。 • 相互认可旨在保护民用航空的各项努力(发展、维护并改进网络安保)。 • 在全球、地区和国家各级推动监管协调，以提高全球协调一致性并确保防范措施的可互用性。 • 在解决国际民航的网络安保方面促进各国的参与。 • 推动并促进网络安保领域的国际活动。 • 认识到网络安保是全球民航系统所有部门的共同责任。

支柱 2 — 治理
• 鼓励、支持和进一步发展国际民航组织网络安保战略。 • 针对民航网络安保制定清晰的国家治理和责任制。 • 确保民航主管部门和相关国家网络安保主管部门之间在国家层面的协调。 • 在各个国家主管部门和业界之间建立适当的协调渠道。 • 将网络安保纳入国家民航安全和安保方案。 • 将网络安保纳入全球和地区计划中。 • 努力达成有关网络安保标准和建议措施的共同基准。

支柱 3 — 有效的立法和规章
• 确保国际法律文书为防范网络事故征候以及起诉肇事者提供适当框架。 • 分析国家现有立法，必要时更新或通过国家立法，以便对影响民航安全、安保、效率或连续性的网络攻击进行防范、调查和起诉。 • 确保已制定了有关民航网络安保的适当国家规章和立法。 • 为国家和业界制定适当的指导原则，以实施与网络安保有关的规定。

支柱 4 — 网络安保政策
• 确保网络安保是民航安全和安保系统以及全面风险管理框架的一部分。 • 确保各种民航网络安保风险评估方法能够保持可比较性。 • 制定虑及航空系统完整生命周期的网络安保政策。

支柱 5 — 信息共享
• 按照现有的国际民航组织规定，建立或利用经认可的信息共享平台和机制，以便感知网络态势，从而能够预防、及早发现和缓解相关网络安保事件。 • 确保向主管当局报告可能对航空安全和/或安保构成重大风险的任何网络事故征候或薄弱性。

支柱 6 — 事故征候管理和应急规划
• 确保制定适当和可扩展的计划，以便在发生网络事故征候时，能保持安全和可靠的民航运营。 • 确保现有应急计划纳入应对网络安保事故征候并从中恢复的规定，并经常/定期进行演习，以测试检测、应对和从网络事故征候中恢复的能力。

支柱 7 — 能力建设、培训和网络安保文化
• 确保航空和网络安保两方面的人员具有承担适当角色的资质。 • 提高网络安保意识，包括制定适当的网络卫生的活动。 • 确保已将适当的航空网络安保课程纳入国家教育框架，以确保包括高级管理层在内的整个组织发展涵盖航空安全和安保的知识体系。 • 推动网络安保创新和适当的研究和开发。 • 将网络安保纳入国际民航组织下一代航空专业人才战略。

第 4 章

实施、监测和审查

4.1 实施

网络安保行动计划的目标是针对国际民航组织、其成员国、业界和其他利害攸关方。鼓励每个实体根据路线图(见附录 A)采纳目标，该路线图概述了优先成果、行动和相关任务。这将有助于国际民航组织、各国和利害攸关方集中精力，努力实施有效措施和行动，以实现建立强有力的全球航空网络安保框架的目标。

4.2 监测和审查

国际民航组织将适时酌情对网络安保行动计划进行审查。国际民航组织还将提供关于网络安保行动计划所列目标和预定最后期限的最新情况。这将包括各国在实施该计划时所需援助领域和所需的能力建设援助领域，以及其他相关努力。

4.3 携手工作

所有航空利害攸关方都需要参与不断改善民航网络安保的努力。网络安保行动计划为所有利害攸关方提供了一个共同的参考框架，并查明了国际民航组织、成员国和业界需要采取的行动，以便制定一个共同的网络安保框架。

4.4 国际民航组织、各国和业界的作用

4.4.1 国际民航组织将在实施和协调网络安保行动计划方面发挥重要的全球领导和监测作用，包括：

- 根据需要，更新网络安保行动计划；
- 制定和保持标准和建议措施(SARPs)及空中航行服务程序(PANS)，辅以手册和其他指导；
- 监测和审查网络安保威胁和风险总体状况；和
- 实施有针对性的援助，以解决民航网络安保的缺陷。

4.4.2 国家和业界也可以为实施网络安保行动计划和保障其有效性发挥重要作用。鼓励各国和利害攸关方在执行该计划方面体现出逐年改进。

第 5 章

国际合作

5.1 编制航空网络安保举措清单

5.1.1 将编制和保持网络安保举措清单，并在国际民航组织门户网站上提供给适当的受众。该清单将汇编现有举措，并涵盖全球、地区或国家层面上有关网络安保的现有航空举措。该清单不仅将虑及航空网络安保举措，而且还将虑及那些结果与民航有关的举措(例如其他运输领域或能源、金融等部门的网络安保)。

5.2 奠定网络安保措施和管理系统互用性的共同基础[2]

5.2.1 国家和业界应制定原则和适当的工具/系统，以确保对信息技术/通信系统的统一、可靠和可互操作的管理。

5.2.2 由于信任是对信息交流进行有效、统一和可互操作管理的基础，因此应支持制定促进信息管理和互操作的国际航空信任框架；此外，所有相关利害攸关方应尽可能地利用政策和程序。

5.2.3 还可通过参与各种形式的国际合作协议来实现网络安保措施和管理的互用性。应该制定一个此类协议的范本，以便开展合作，同时遵守适用的隐私、信息安全和国家安保政策。在此方面，需要确定下列方面作为协议范本的基准：

- 协议主题和目标；
- 可以缔结此类协议的实体；
- 这些实体的作用和责任；和
- 可用于改善民航网络安保并需加以协调的措施。

5.2.4 国际协议的宗旨应是：

- 在各利害攸关方之间建立对话，讨论降低集体风险和保护国家和国际民用航空基础设施的方法；
- 减少和缓解风险的措施，以应对民航面临的网络安保威胁；
- 就与网络安保相关的国家民航立法、国家战略、政策和最佳做法交流信息；和
- 根据需要，支持网络安保能力建设的措施。

[2] 此范畴内的管理系统包括但不局限于风险管理体系。

5.2.5　鉴于航空利害攸关方可能各有许多方法论原则和模型，所用词汇可能也各不相同，重要之处在于制定共同的词汇和理解框架，特别是在民航网络安保方面。在此方面，必须与成员国和业界密切合作，在国际民航组织一级进一步制定关于全球协调适当管理网络安保风险的一套总体原则。将对现有的框架进行分析，以确定用以实现无缝隙有效统一这些原则和模型的最佳方式。

5.3　编制通用术语

5.3.1　将在国际民航组织主持下制定有关民航网络安保的通用术语，并考虑到与网络安保相关的现行术语和航空相关术语和框架，以使所有航空利害攸关方无论其背景和活动水平如何均可以相互理解。

5.3.2　目标旨在促进网络安保相关活动。这并不意味着将为所有术语确定和/或商定一个单一的定义。对于同一术语(例如，可能性、严重性、发生等)存在各种定义是可以接受的，前提是它们是基于具体上下文的，并且这种重复不会产生混淆，可能造成对民航网络安保风险的无效管理。具体而言，随着对综合安全和安保风险管理的日益重视，国际民航组织必须密切关注确保对术语进行正确统一。回顾上述初始背景综述，并且忆及需要澄清的一方面是在管理非法和故意行为方面确保安保，而另一方面是涉及故意、非故意和随机危险方面的安全，因此需要对可能涵盖安保和安全两方面关切的综合风险管理问题进一步加以完善处理(国际民航组织附件 17 和附件 19 的定义可作为基准使用)。具体而言，由于安全和安保学科的重点不同(安全着重于故意、非故意或随机的危险，安保着重于非法和故意行为)，实行跨两个学科的综合风险管理就需要明确所用术语的范围和目的。

5.4　制定通用的航空信息交换/互动图

5.4.1　制定一个通用框架，用以确定描述各航空行动者之间信息交换的高级别功能图，是确保了解总体网络风险状况的一项必要先决条件。需要一个通用框架，以确定所有航空利害攸关方之间信息交换的高层面映射图，以了解总体网络风险状况。

5.4.2　这种高层面信息交换/互动映射图的通用性应足以涵盖所有航空相关类型的运行，并且应该尽可能独立于已实施的物理和/或技术架构(功能/服务方法)。例如，高层面映射图应涵盖空中交通管理和机场相关活动的数字数据流，以及从事飞行/维护运行的航空器的数字数据流。这一高层面图应该利用其他群组已着手开展的任何现有工作。其目的是允许每个利害攸关方完成/调整/定制各自的交流互动图，以了解其如何与其他利害攸关方进行互动。最终每个利害攸关方应能根据自己独特的情况制定或调整这一映射图。因此，可以尽可能与其他利害攸关方交换/共享每个行动者使用自己的方法和标准进行安保风险评估的结果(基于共同风险评估框架可以互比的方法和标准 — 见第 5.6 节)。通过合作，利用可比较的安保风险评估框架并使用信息交换/互动图，利害攸关方将能了解到，风险如何能够进一步传播给其他风险共享伙伴或由这些伙伴管理，从而允许共享关于每个利害攸关方产生或诱发的风险的信息。

5.5 开展组织间风险信息共享

5.5.1 许多标准和指导文件都处理了每个组织对其自身网络安保管理的责任，涉及内部系统、过程、产品和数据。然而，鉴于民航的网络安保风险是多个利害攸关方共同承担的，因此有必要超越单个组织。为了有效和高效地实现共享风险管理，必须强调要共享风险信息，这是系统、过程、产品或数据共享或在组织之间传递情况下所必需的。

5.5.2 应考虑与第三方供应商达成外部协议，以实现组织与相关当局/监管机构之间共享敏感的网络安保信息，以促进对供应链风险和威胁的管理。

5.6 界定风险评估态势的兼容性标准

5.6.1 在风险跨越多个组织的背景下，至关重要的是，利害攸关方能够理解端到端风险以及其他利害攸关方对这些风险管理的相关风险承受能力。在这种情况下，应制定便于理解和比较网络安保风险评估的标准。

5.7 开展适当的民用和军用协调

5.7.1 在可能的情况下以及符合国家法律包括但不限于国家安保和国防规定的情况下，民航和军事主管部门应建立能力和流程，在与航空网络安保相关的事项上进行合作。

5.7.2 民用和军用航空利害攸关方之间从早期就适当分享和协调与网络安保有关的信息，对查明潜在的网络威胁和风险非常有益，从而有助于成功缓解航空系统的网络风险。

5.7.3 民用和军用航空利害攸关方之间的信息共享对于管理网络安保危机也很重要。各国可支持本国的民用航空和军用利害攸关方在实际可行的范围内达成安排，通过适当机制促进信息共享。

5.8 促进全球和地区民航网络安保活动

5.8.1 国际民航组织将酌情支持和计划举办促进民航网络安保的全球和地区活动。

第 6 章

治理

6.1 建立治理结构

6.1.1 国际民航组织应建立航空网络安保的内部治理结构，确保对所有相关航空领域和专业领域的网络安保和网络复原力采取全面、跨领域和基于风险的方法。

6.1.2 此外，各国应确定和实施民用航空网络安保的国家治理和问责结构，确保制定和实施国家和国际网络安保和网络复原力的规定，并确定每个利害攸关方在国家层面的作用和责任。这种开发还应考虑到国家民用航空和网络安保主管当局之间所需的协调。

6.2 制定网络安保多年度计划

6.2.1 建议将网络安保行动计划(CyAP)与现有的全球航空安保计划(GASeP)、全球空中航行计划(GANP)和全球航空安全计划(GASP)进行适当统一，应该在这些计划中酌情纳入并促进网络安保方面的内容。

6.2.2 为了确保全球计划的适当国家实施和应用，敦促各国将国家协调和相应的网络安保相关行动纳入其国家安全和安保方案以及空中航行计划。

6.3 建立治理和责任制

6.3.1 国际民航组织应制定网络安保政策指南，以促进全球、地区和国家网络安保政策的协调和一致。

6.3.2 网络安保治理应是政策驱动的和强制执行的，并且需要确定遵规责任。

6.3.3 各国应采取切实行动，持续提高国家一级网络安保管理进程的效率、质量和一致性。

6.3.4 如有必要，信息安保管理系统(ISMS)可以成为管理网络安保的有效工具，并且可以在国家或组织层面实施。[3]

[3] 在建立国家一级的网络安保治理时，各国可从 ISO 27001 中汲取灵感，确定领导原则，例如：确保将信息安保管理系统要求纳入组织进程之中；确保可以获得所需资源；并确保信息安保管理系统达到预期效果。

第 7 章

有效的立法和监管框架

7.1 对有关网络安保领域的现有国际航空法文书的审查

7.1.1 国际民航组织将对现有国际航空法文书进行分析，查明与网络风险有关的现有和可能漏洞，并提出可能的解决办法，填补查明的可能漏洞，以进一步保护民用航空。

7.2 使国际民航组织规定与网络安保需求保持一致

7.2.1 随着航空网络安保日臻成熟，可能需要制定规定来完善或补充现行标准和建议措施(SARPs)和航行服务程序(PANS)。应该在个案基础上开展这一工作，同时注意到应尽最大可能避免增加标准和建议措施以及航行服务程序的新规定，并根据需要，在所有相关利害攸关方之间进行协调。

7.3 《北京公约》和《议定书》的批准

7.3.1 鼓励各国批准《制止与国际民用航空有关的非法行为公约》(2010 年北京公约)和《制止非法劫持航空器公约补充议定书》(2010 年北京议定书)。

7.4 各国确保在国家一级制定和实施适当的立法和规章

7.4.1 鼓励各国评估其网络安保和民航领域的国家现行法律框架，以确定现有的差距，并确保针对具体的民航网络安保内容落实适当的立法和规章。另一个关键要素就是鼓励其国家法律框架中仍没有执法机制的国家建立执法机制，以便对使用网络手段针对民用航空的非法行为进行刑事定罪和追诉。

第 8 章

网络安保政策

8.1 制定和实施网络安保政策

8.1.1 需要在国家和组织各级制定网络安保政策。各国应制定明确可行的网络安保政策，其中包括：

- 根据民航网络安保风险评估结果制定的目标；
- 关于满足适用要求的承诺和评估合规的方法；
- 关于管理外部依赖方并与其协调方面的考虑因素(见国际合作一章)；
- 对不断改进网络安保框架的承诺；
- 确保政策完全形成文字并可作为官方信息予以提供的规定；和
- 确保政策得到适当传播的规定。

8.2 查明和评估民航网络风险

8.2.1 风险识别和评估活动的挑战之一是能够预见到威胁的来源和特性的迅速变化。对不断变化的威胁作出预期至关重要，以帮助航空运输系统不仅根据当前的威胁，而且根据未来的潜在威胁，积极主动地调整其防范战略。拜这一预期所赐，虽然攻击一方灵活性和适应性很强，而防守一方受所需保护的系统复杂性之累反应迟缓，在这种灵活性不对称情况下，民航部门应能做到更积极主动行事。在这种情景之下，这一积极主动的做法愈加至关重要。因此，有必要制定一个网络安保风险查明和评估框架，以支持帮助减缓这些风险的需要。

8.2.2 建议查明和评估网络安保风险，同时虑及攻击民航系统的所有潜在后果(安保、安全、有效、复原力、服务连续性等)以及所有潜在威胁来源以及存在这种威胁的薄弱性。这项活动应以先前在航空安保专家组威胁和风险工作组(WGTR)主持下制定的网络风险矩阵为基础。

8.2.3 由于民航网络安保的很大一部分风险是由许多利害攸关方共同承担的，建议考虑制定航空信息交换/互动映射图(见第 5.1 章)。必须将这张映射图视为一种手段，用以保证所考虑的情景是详尽无遗的，并使利害攸关方了解到他们彼此如何互动以及他们对风险的依赖性。

8.2.4 由于网络安保风险的严重程度将随着时间的推移而变化，这些风险较之其他风险可能更迅速地演变，建议考虑采用能够迅速协调部署的办法，调整全球航空对这些风险的响应(例如，在航空标准、指导材料、非航空最佳做法之间实现需求平衡，并利用/依赖其他领域的响应情况)。

8.2.5 建议查明和评估网络安保风险的活动完全由民航网络安保专家组成的专家组予以开展和协调，或由网络和民航专家组成的团队开展和协调，这些专家最好是在网络安保领域具有广泛经验的专家。

8.2.6　　这组专家应该负责拟定一份全球网络安保风险背景综述。

第 9 章

信息共享

共享与网络安保有关的信息是管理民用航空系统网络安保风险的关键。由于认识到促进信息共享是建设网络安保文化的一个关键因素，民航利害攸关方应制定和利用并尽可能实施能够在其组织内和与外部各方共享信息的方案。它们应通过这些方案发展伙伴关系，与拥有和运营民航基础设施的其他利害攸关方分享实质性信息，并在其组织内制定信息共享计划和做法。

这些信息共享方案应能促进针对已知和新出现的网络威胁来制定、运行和调整民航网络防御。它们应有助于发展：

- 在日常正常运行情况下和在发生危机、事故征候或事件期间的情景意识；
- 运行和策略风险管理以预测和应对威胁；
- 能力建设的战略规划，以增强未来网络安保和复原力。

9.1 开展风险信息共享

9.1.1 网络相关信息的共享具有双边和多边两个层面，是以下各方之间(国家、地区、全球)交汇的任何组合：

- 国家网络主管部门；
- 国家民航主管部门；
- 国家军用航空主管部门；
- 其他航空利害攸关方(运营人、服务提供者和制造商)；和
- 非航空利害攸关方(IT 和通信服务提供者和供应链)。

9.1.2 人们认识到，与网络安保有关的信息种类多样，例如：

- 网络情报，例如总体威胁情况、网络威胁行为者的能力和意图的情报。
- 危害指标(IoCs)。
- 战术、技术和程序(TTP)，例如攻击情景和黑客使用的首选方法。
- 薄弱性，例如硬件、软件、服务、协议、标准等，包括潜在的利用场景。
- 事故征候报告。

9.1.3 根据国家立法和网络相关信息的性质而定，在与各种信息接收者(如国家网络管理部门、国家民用航空管理部门、国家军用航空管理部门和其他航空利害攸关方)共享信息方面，可能存在各种共享方法和限制。

9.1.4　应在全球、地区和国家各级确定信息共享、协作需要(包括但不限于危机时期)和政策。

9.1.5　建议在分发和进一步共享网络相关信息时，使用交通信号灯规程(TLP)[4]来说明分发/限制的级别。

9.1.6　网络相关信息可能包含一些敏感信息，在共享之前应该尽可能去除标识或消毒，而不是完全不共享。

9.2　制定安保研究员责任披露原则和指南

9.2.1　鉴于安保研究人员群体对民航网络安保的兴趣日益浓厚，为了避免不负责任地披露可能对民航的安全、安保、效率或连续性有害的调查结果，需要确定负责任地披露安保研究人员或第三方所发现的薄弱性的原则，以确保这些披露不会损害民航网络安保。这应虑及《网络安保战略》建议 4.4。

9.2.2　应该制定关于这些原则(例如发现、制造商通知、调查、解决、业界通知和最后公开发布等其他关切)的指导方针，受众一方面是研究人员和第三方，另一方面是航空主管部门和航空利害攸关方，以最大程度确保此类薄弱性研究/发现和披露活动对安全和服务的提供不会产生影响。理想上而言，有关指导不仅涉及负责任的披露过程，而且还包括增强意识和教育因素。

9.3　为民航目的发展全球范围内地区/国家网络主管部门网络

9.3.1　国家和行业内部的网络安保责任并不是统一分配的，相关专长分布于广泛的航空和非航空利害攸关方和职能领域当中。这种多样性产生的固有关切就为查明实体内适当的联系人并在各利害攸关方之间建立和保持正式沟通渠道带来了困难。指导各国和各组织就民航网络安保相关事项建立和保持单一联系人，有助于建立全球、地区和国家沟通渠道，建设相关的网络安保界并推动网络安保文化。

9.4　全球航空网络安保信息共享能力

9.4.1　可在全球、地区和/或国家各级横向发展民航信息共享能力，以促进交流网络安保相关信息。

9.4.2　信息共享论坛可能包括公共 — 公共、公共 — 私营和私营 — 私营结构。利害攸关方应参与受信任的社区，以促进最佳做法和威胁情报的交流。

[4] 参见国际民航组织关于“交通信号灯规程”的指导材料。

第 10 章

事故征候管理和应急规划

10.1 发展事故征候响应能力和应急响应规划

10.1.1 强烈鼓励所有利害攸关方与其运行伙伴一起协调制定和测试事故征候响应和应急计划，其中包括：

- 利用已经制定的现有应急计划和/或修改这些计划，将网络安保的规定纳入其中；
- 民航利害攸关方制定并保持适当的可扩展性，以便在可能发生网络事故征候期间，保持航空运输运行的安全、安保和连续性；
- 制定网络安保事故征候应对和恢复能力的规定，包括突发和应急响应预案；
- 使军用航空利害攸关方参与规划进程，积极建立沟通渠道；
- 达到可接受的绩效水平，并满足维持基本服务最低服务水平的要求；
- 制定网络事故征候报告的统一分类，并协调在国家、地区和如适用在国际层面的民航网络安保事故征候报告机制；和
- 航空利害攸关方应定期进行现场演练，以测试在规划和桌面演练中所做各种假设的有效性。

10.2 利害攸关方层面的事故征候发现、分析和响应手段

10.2.1 应尽可能实施事故征候响应计划，各级利害攸关方应制定关于网络安保事故征候发现、分析和响应的能力。重要的是监测这些对于支持民用航空至关重要的系统/服务的网络安保状况，以便发现潜在问题并跟踪安保防范措施的持续有效性。一旦发现网络安保事故征候，应进行分析，并实施适当的响应计划；这些计划应包括减轻网络安保事故征候影响的行动。

10.3 建立民航网络安保危机协调小组

10.3.1 应在可能范围内实施具备民航网络安保专长的民航危机协调小组(建立在现有的机制之上)，并酌情使军用航空利害攸关方也参与其中。

10.3.2 应在业界所有利害攸关方参与的情况下，酌情定期进行演练，特别是桌面演练(TTX)。

第 11 章

能力建设、培训和网络安保文化与教育

11.1 制定技术能力、培训和网络安保文化与教育材料

11.1.1 应在全球、地区和国家各级界定和促进民航网络安保教育、培训和提高意识活动。

11.1.2 网络安保文化和教育活动应由高级管理层在各个民航机构内加以推广，并应突出强调不同行动者的重要作用及其期望。它应促使建立一个涵盖航空安全和航空安保的网络安保知识体系，并应包括：

- 与安全界协调减缓网络威胁的撼按设计安保攡原则概念。这些概念应有助于航空安全界在应对网络威胁时作出更知情的决定；
- 安保和安全利害攸关方之间的协调做法，并认识到安保控制措施不得对飞行安全产生不利影响，使技术知识的转移成为可能，以及确保根据相互理解的全面风险情况作出知情的决定；
- 关于运营和支助人员的网络卫生做法的概念，有助于防止由于撼商用现货攡(COTS)产品和非特定恶意软件数量的增加对民航系统造成潜在不利影响；和
- 安全界的“公正文化”概念，以实现和促进人员自我报告由于非故意行为(如处理 U 盘时的意外不当行为)所造成的事故征候。

11.1.3 在开展这些活动时，应将重点放在影响/潜在影响方面。

11.1.4 这种网络安保文化的发展和网络安保文化与教育材料的推广应有助于在安全和安保界形成对网络安保风险状况的相互/共同理解，以及对正在采取的对策的相互信任。

11.1.5 国际民航组织应鼓励跨国家/跨地区的网络安保教育和培训交流计划。[5]

11.1.6 网络安保文化和教育活动不仅应着重于各个系统的运行，而且更应侧重于整个系统生命周期，包括：

- 需求(安保已经成为需求阶段的组成部分)；
- 设计(根据设计安全战略，硬件、软件和数据的安保、变更管理、薄弱性管理)；
- 开发(可靠的环境、持续和集成的安保测试)；
- 制造/购买(包括信息和运营技术的硬件和软件供应链)；
- 运行(包括访问管理、数据完整性、可靠的系统操作)；

[5] 例如跨国公司举措或欧盟网络安保能力网络和中心举措。

- 维护(包括修补和更新战略)；和
- 处置(包括对证书和存储装置上的残余数据的管理)。

第 12 章

结论

《网络安保行动计划》将国际民航组织、各国、业界和其他利害攸关方聚集在一起，进行全面和协调的努力，应对当前和新出现的网络安保挑战。该计划突出强调，网络安保是一个贯穿航空业所有领域的跨部门问题。该计划有助于实施国际民航组织航空网络安保战略，并朝着创建一个强而有力的全球网络安保框架迈进。

— — — — — — — —

附录 A

网络安保行动计划路线图

网络安保战略总体行动

优先成果	制定一项获得一致认同的全球愿景				
优先行动	• 认识到目前迫切需要制定一项全面的、获得一致认同的网络安保愿景，作为稳固和协调一致的全球航空网络安保风险管理的基础。 • 认识到民用航空业须善于应对网络攻击，在全球保持安全并得到信任，同时保持创新和增长。 • 认识到需要按照《国际民用航空公约》处理民航网络安保风险。				
行动					
行动编号	行动实体	具体措施/任务	指标	优先程度	实施开始日期
CyAP 0.1	国际民航组织、成员国和业界	国际民航组织制定网络安保政策范本，供成员国和业界在制定自己的国家/组织政策时参考。	范本供成员国和业界使用。	高	2021
CyAP 0.2	国际民航组织和成员国	在国家一级(按照大会 A40-10 号决议的指示)开始实施国际民航组织航空网络安保战略的工作(为核查各国在战略实施方面的状况，需制定用以衡量若干行动实施情况的一整套衡量指标)。	国家展开实施工作的证据。	高	2023
CyAP 0.3	国际民航组织	开展问卷调查，确定各国在实施国际民航组织航空网络安保战略方面的状况。(问卷调查将询问各国是否制定了实施这一战略的行动计划)	国际民航组织发给成员国的问卷调查/问答卷。	高	2021-2022

网络安保战略支柱

优先成果	**1.** 实现国际合作
优先行动	• 在国家、地区和国际层面所有利害攸关方之间开展合作。 • 相互认可旨在保护民用航空的各项努力(发展、维护并改进网络安保)。 • 在国际、地区和国家各级推动监管协调，以提高全球协调一致性并确保防范措施的可互用性。 • 在解决国际民航的网络安保方面促进各国的参与。 • 推动并促进网络安保领域的国际活动。 • 认识到网络安保是全球民航系统所有部门的共同责任。

行动

行动编号	行动实体	对航空网络安保战略的可追溯性	对第 5 章的可追溯性	具体措施/任务	指标	优先程度	实施开始日期
CyAP 1.1	国际民航组织和成员国	1.1	5.2	将网络安保纳入国际民航组织安全和安保监督计划 — 将相关标准纳入国际民航组织审计计划(例如普遍安全监督审计计划(USOAP)和普遍安保审计计划(USAP))。	国际民航组织安全和安保这两方面的审计计划都包含了网络安保的相关标准。	高	持续进行
CyAP 1.2	国际民航组织	1.1	5.1 也参见 CyAP 4.6(行动计划第 8.2 段)	开展网络安保举措/做法的问卷调查，确定各国和业界如何管理民用航空网络安保。	问答卷结果，举措的数目和地区。	高	持续进行
CyAP 1.3	国际民航组织	1.1	5.1	编制国际民航组织各个专家组所参与的所有网络安保举措的清单。	国际民航组织航空网络安保工作方案由特设网络安保协调委员会制定和维护。	高	2024

CyAP 1.4	国际民航组织和成员国	1.2	5.2.3 和 5.5 也参见 CyAP 5.1（行动计划第 9.2 段）	A) 制定谅解/协作备忘录、外部协议的模板。 B) 提供如何制定这些协议的指南。	提供模板和指南。	低	2023-2024
CyAP 1.5	国际民航组织、成员国和业界	1.2	5.3	制定有关民用航空网络安保的一致同意的通用术语，使各航空利害攸关方（无论其背景和活动水平如何）均可以在网络安保方面相互理解。	发布网络安保词汇表。	中度	2023
CyAP 1.6	国际民航组织、成员国和业界	1.2	5.4	国际民航组织制定一个通用框架，用以确定描述各航空行动者（如： 空中航行服务提供者（ANSP）、航空公司运行中心（AOC）、空管、机场、气象部门（MET）、机务维修机构（MRO）、通信、导航和监视（CNS））之间的信息交换的高级别功能图，作为促进了解总体网络风险状况的必要条件。 成员国和业界在国家和机构各级制定此种框架。	存在通用框架和已确定的有关航空信息交换/互动的通用总图。 认识和理解功能图。	高	2024
CyAP 1.7	国际民航组织和成员国	1.2	5.7 也参见 CyAP 6.2 和行动计划第 10.2 段	国际民航组织将制定民用和军用航空之间的合作模式，以便酌情为民用和军用可互用航空接口制定模型/指南。 确定适当互动的标准和水平。	提供民用/军用网络合作和可互用性模型/指南。 已发布的标准和所需最低程度互动的列表。	高	2023
CyAP 1.8	国际民航组织、各成员国和业界	1.3	5.8	规划、组织和支持促进民航网络安保的全球和地区活动。	活动、意识建设、国际合作。	不适用	持续进行

CyAP 1.9	国际民航组织、成员国和业界	1.3	5.4	确保所有利害攸关方都参与有关民用航空网络安保的讨论和活动。 加强相关利害攸关方的持续参与和联络工作。	发布共同努力的结果。 发布参与的证据，例如伙伴关系、小组成员资格等。	高	持续进行
CyAP 1.10	国际民航组织、成员国和业界	1.2	5.2.2	制定一个国际航空信任框架，帮助各实体基于其对其他利害攸关方建立的信任关系实现互用性。	制定可供许多机构使用的信任框架。	高	2024-2025

优先成果	**2. 建立治理和责任制**
优先行动	• 鼓励、支持和进一步发展国际民航组织网络安保战略。 • 针对民航网络安保制定清晰的国家治理和责任制。 • 确保民航主管部门和相关国家网络安保主管部门之间在国家层面的协调。 • 在各个国家主管部门和业界之间建立适当的协调渠道。 • 将网络安保纳入国家民航安全和安保方案。 • 将网络安保纳入全球和地区计划中。 • 努力达成有关网络安保标准和建议措施的共同基准。

行动

行动编号	**行动实体**	**对网络安保战略的可追溯性**	**对第 6 章的可追溯性**	**具体措施/任务**	**指标**	**优先程度**	**实施开始日期**
CyAP 2.1	国际民航组织和成员国		6.1	制定民航网络安保领域的治理结构。	查明民航网络安保的适当治理结构。	不适用	2021-2023
CyAP 2.2	国际民航组织和成员国	2.2	6.3	国际民航组织制定一套关于适当管理民航网络安保的总体原则。成员国按照国际民航组织模式，在国家一级制定这些原则。	发布总体原则。	高	2023-2024

CyAP 2.3	国际民航组织、成员国和业界	2.2	6.3.2 也参见行动计划第 8.1 段	制定指导材料以支持各组织实施协调一致的网络安保管理框架，以支持建立管理航空网络安保风险的系统方法并评估这些框架的成熟度和有效性。	发布指导原则。	高	2023
CyAP 2.4	国际民航组织和成员国	2.2	6.3	促进民航主管部门和网络安保主管部门之间的协作机制。	国际民航组织问卷调查 — 查明已实施协调机制数量。	中度	2022
CyAP 2.5	国际民航组织	2.3	6.2.1 也参见 CyAP 1.9(行动计划第 5.2 段)	国际民航组织将网络安保纳入地区和全球计划，以确保航空的安全、安保和复原力。	发布经更新的计划。	不适用	2022-2023
CyAP 2.6	国际民航组织		6.2	国际民航组织在信息库中编拟最佳做法汇总/指导原则部分。	国际民航组织最佳做法信息库。	不适用	2020-2021
CyAP 2.7	国际民航组织、成员国和业界	3.2	6.3	国际民航组织制定关于报告网络事故征候的示范程序，包括事故征候分类指南。 成员国和业界及时和有效地制定关于报告网络事故征候的国家和机构程序。	网络事故征候报告程序/按照程序报告的事故征候数量。	高	2022-2023
CyAP 2.8	国际民航组织和成员国	2.2	6.2	国际民航组织评估成员国将网络安保纳入其国家民用航空安全和安保方案和空中航行计划的程度。	国际民航组织问卷调查 — 已将网络安保纳入其国家民航安全和安保方案的国家数目。	高	2022 年问卷调查 进一步行动持续进行

优先成果	**3. 制定有效的立法和规章**
优先行动	• 确保国际法律文书为防范网络事故征候以及起诉肇事者提供适当框架。 • 分析国家现有立法，必要时更新或通过国家立法，以便对影响民航安全、安保、效率或连续性的网络攻击进行防范、调查和起诉。 • 确保已制定了有关民航网络安保的适当国家规章和立法。 • 为国家和业界制定适当的指导原则，以实施与网络安保有关的规定。

行动

行动编号	行动实体	对网络安保战略的可追溯性	对第 7 章的可追溯性	具体措施/任务	指标	优先程度	实施开始日期
CyAP 3.1	成员国	3.3	7.4	成员国批准北京文书。	已批准北京文书的国家数目。	高	持续进行
CyAP 3.2	国际民航组织	3.3	7.3	分析国际航空法律文书。	审查和差距分析相关国际航空法律文书。	高	2022
CyAP 3.3	国际民航组织和成员国	3.3 和 3.4	7.2	分析民航网络安保领域现有国内立法并查明差距，包括刑法。	调查关于处理通过网络手段实施的针对民用航空的非法行为的国家立法状况。	中度	2023-2024
CyAP 3.4	国际民航组织	3.3	7.1	审查国际民航组织现有标准和建议措施，查明可能的网络安保更新需求。	审查和差距分析国际民航组织的标准和建议措施。	高	2022
CyAP 3.5	国际民航组织	3.2		制定、审查和修订关于实施民航网络安保要求的指导材料。	出版民航网络安保指导材料。	高	2021 年和持续进行

优先成果	**4. 制定网络安保政策**
优先行动	• 确保网络安保是民航安全和安保系统以及全面风险管理框架的一部分。 • 确保各种民航网络安保风险评估方法能够保持可比较性。 • 制定虑及航空系统完整生命周期的网络安保政策。

行动

行动编号	行动实体	对网络安保战略的可追溯性	对第 8 章的可追溯性	具体措施/任务	指标	优先程度	实施开始日期
CyAP 4.1	成员国和业界	4.1	8.1	成员国和业界确保其管理层致力于解决民用航空网络安保和网络复原力的承诺。	增强意识的活动/承诺的证据，例如承诺声明、在当局和机构的管理手册中明确规定了网络安保领域的职责。	中度	2022-2023
CyAP 4.2	国际民航组织、成员国和业界	4.3	8.2 也参见行动计划第 5.11 段	通过与大学、研究所、研究团体等携手工作，鼓励民用航空的网络安保研发。	互动次数和项目数量。	高	2022-2023
CyAP 4.3	成员国和业界	4.2	5.6 和 8.2	在信息共享的同时，制定共享的跨机构风险评估的标准以及开展风险比较所需的标准。 界定成员国在国家一级和业界在机构一级此类标准。	公布共享的跨机构风险评估目标和标准。	高	2023
CyAP 4.4	国际民航组织、成员国和业界	4.3	8.1	制定按设计制定的安保政策，作为可靠的民航系统生命周期的基础。	拟定可靠的民航系统生命周期政策。	中度	2022-2023

CyAP 4.5	国际民航组织、成员国和业界	4.2	8.2	国际民航组织建立旨在讨论跨机构/跨职能的网络安保和网络复原力目标以及最低水平的民航部门基本职能的国际论坛。 成员国在国家和地区一级建立此类论坛，业界建立专门论坛，并积极参与国际民航组织和成员国建立的论坛。	讨论目标的论坛数目。	高	2022-2023
CyAP 4.6	国际民航组织、成员国和业界	4.3	8.2	制定现有的民航网络安保风险管理举措清单(包括风险形态、情景、薄弱性管理和风险评估)。	提供网络安保风险管理举措信息库。	中度	2023-2024
CyAP 4.7	国际民航组织、成员国和业界	4.3	8.3	国际民航组织在国际一级制定网络风险战略情景列表。成员国和业界在国家和机构各级作出投入并编制类似列表。	提供 10 个网络风险情景。	高	2023-2024
CyAP 4.8	国际民航组织、成员国和业界		8.2	国际民航组织制定每个运行领域的风险形态。 成员国和业界在国家和机构各级通过制定类似风险形态来作出投入。	提供风险形态。	高	2023
CyAP 4.9	国际民航组织		8.2	拟定全球网络安保风险背景综述。	发布全球网络安保风险背景综述。	高	2023

优先成果	5. 发展信息共享能力
优先行动	• 按照现有的国际民航组织规定，建立或利用经认可的信息共享平台和机制，以便感知网络态势，从而能够预防、及早发现和缓解相关网络安保事件。 • 确保向主管当局报告可能对航空安全和/或安保构成重大风险的任何网络事故征候或薄弱性。

行动

行动编号	行动实体	对网络安保战略的可追溯性	对第 9 章的可追溯性	具体措施/任务	指标	优先程度	实施开始日期
CyAP 5.1	国际民航组织	5.1	9.1 和 9.2	国际民航组织编制信息共享指南。	向安保界提供信息共享指导文件。	高	2022-2023
CyAP 5.2	国际民航组织	5.1	9.1	国际民航组织在成员国和业界支持下，查明涉及网络安保的信息共享、协作需求（包括但不限于危机时刻）和政策。	制定可能共享的信息列表。	中度	2022-2024
CyAP 5.3	国际民航组织	5.1	9.1	在分发和进一步共享网络信息时，编制使用交通信号灯协议（TLP）说明分发/限制等级指南。	公布关于分发和共享网络信息时使用交通信号灯协议的政策指南。	高	2021
CyAP 5.4	国际民航组织、成员国和业界	5.2	9.2	审议制定负责任地披露网络安保薄弱性标准的可行性。	在可行的情况下，提供并发布有关负责任地披露薄弱性的原则。	高	2023
CyAP 5.5	国际民航组织和成员国	5.2	9.4	国际民航组织在国际一级为各成员国和业界制定并保持一个民航网络安保相关事项的联系人网络。 成员国与国际民航组织合作，在国家一级建立这种联系人网络。	建立民航网络安保联络人网络。 公布每个成员国的联系人网络。	中度	2024-2025

优先成果	**6. 制定事故征候管理和应急规划**
优先行动	• 确保制定适当和可扩展的计划，以便在发生网络事故征候时，能保持安全和可靠的民航运营。 • 确保现有应急计划纳入应对网络安保事故征候并从中恢复的规定，并经常/定期进行演习，以测试检测、应对和从网络事故征候中恢复的能力。

行动

行动编号	行动实体	对网络安保战略的可追溯性	对第 **10** 章的可追溯性	具体措施/任务	指标	优先程度	实施开始日期
CyAP 6.1	成员国和业界	6.1	10.1	成员国制定有关民航部门基本功能的目标和最低水平。 业界采用制定的目标。	公布航空连续性目标和可接受功能的最低水平列表。	高	2022-2023
CyAP 6.2	国际民航组织和成员国	6.1	10.2	国际民航组织制定关于将军队利害攸关方纳入民用航空网络安保事故征候响应规划的指南和流程。 成员国制定民用航空当局与军事航空当局合作的程序和协议。	制定和发布民航网络安保事件响应中军民合作流程和程序的指南。	高	2022-2023
CyAP 6.3	国际民航组织、成员国和业界	6.1.	10.1	国际民航组织制定有关民航网络事故征候响应和复原能力指南，包括突发和应急响应预案。 成员国和业界遵循国际民航组织的指导，在国家和机构各级制定这种指南。	公布有关民航网络事故征候响应和复原能力指南，包括突发和应急响应预案。	高	2022-2023
CyAP 6.4	成员国	6.1.	10.2 和 10.3	成员国制定和实施在运行层面有关民航网络安保事故征候的检测、分析和响应的能力和方案。	调查以跟踪实施水平。	高	2023-2024
CyAP 6.5	国际民航组织和成员国	6.1.	10.1	在国家和国际各级制定有关民航网络安保危机协调的流程。	界定建立的网络安保危机协调流程。 发布指导材料。	中度	2024-2025
CyAP6.6	成员国和业界	6.1	10.3	定期进行桌面演练和现场演练。	酌情分享汲取的经验教训。	高	2022-2023

优先成果	**7. 发展能力建设、培训和网络安保文化**
优先行动	• 确保航空和网络安保两方面的人员具有承担适当角色的资质。 • 提高网络安保意识，包括制定适当的网络卫生的活动。 • 确保已将适当的航空网络安保课程纳入国家教育框架，以确保包括高级管理层在内的整个组织发展涵盖航空安全和安保的知识体系。 • 推动网络安保创新和适当的研究和开发。 • 将网络安保纳入国际民航组织下一代航空专业人才战略。

行动

行动编号	行动实体	对网络安保战略的可追溯性	对第 11 章的可追溯性	具体措施/任务	指标	优先程度	实施开始日期
CyAP 7.1	国际民航组织、成员国和业界	7.1.	11.1	界定并促进民航网络安保文化和教育。	提供与民航网络安保文化有关的课程和指导材料。	中度	2022-2023
CyAP 7.2	成员国和业界	7.2.	11.1	成员国和业界制定其机构内具有适当作用的各级民航网络安保培训需求。	开办具有适当作用的民航网络安保培训。	高	2022-2023
CyAP 7.3	国际民航组织和成员国	7.3.	11.1	国际民航组织将网络安保纳入下一代航空专业人才战略。 成员国将网络安保纳入其与下一代航空专业人才战略相关的国家战略。	将网络安保纳入下一代航空专业人才战略。	中度	2022-2023
CyAP 7.4	国际民航组织	7.3.	11.1	国际民航组织分析支持具有网络安保作用的能力要求的手段和方法。	将具有网络安保作用的培训纳入国际民航组织 Doc 7192 号文件和 Doc 9868 号文件。	高	2023-2025
CyAP 7.5	国际民航组织、成员国和业界	7.3.	11.1	开展能力建设活动。	提供民航网络安保培训课程。	高	持续进行

— 完 —