网络安保政策指南

由秘书长授权出版

2022 年 1 月

国际民用航空组织

1. 引言

本指南系根据国际民航组织航空网络安保战略[1]和网络安保行动计划[2]编写，其中行动项目 CyAP0.1 建议国际民用航空组织(ICAO)编写网络安保政策范本，供各成员国和业界制定国家/内部政策时参考。

该网络安保政策范本载于本指南附录 A。

2. 范围

本文件附录 A 概述的网络安保政策范本述及保护国际民用航空的关键基础设施免受网络威胁及其应变能力，以及民用航空内部及其与军事、网络安保和国家安全等外部当局之间的多边合作要求。

3. 目标

本网络安保政策范本旨在用作指南，帮助各国和业界聚焦于资源和行动，对民用航空网络安保(包括现有系统和旧系统)采用系统做法。最终目标是使各国和利害攸关方能够制定一种保护民用航空可免受网络威胁、及时应对网络事故征候并从中恢复的系统之系统做法，从而抵御新的威胁，而不会发生重大服务中断。

执行网络安保政策的主要预期成果是：

3.1 确保民用航空免受网络威胁

通过实施国际民航组织网络安保标准和建议措施、程序和指导材料，保护民用航空免受网络攻击，其中包括采用强有力的风险管理做法，查明关键基础设施，以及采用全面的多层面网络安保做法。该做法应确保对某一层面攻击的得手不会损害系统其他层面和/或造成关键功能的安全、安保或连续性丧失。该系统还应采用一种持续改进做法，确保协调并落实规划技术或程序演变的必要改进并保持更新。

3.2 确保民用航空具有网络复原力

具有网络复原力的民航系统是指在受到攻击情况下能够保持关键功能的系统，即支持安全和安保的、干扰最小(如有)的飞行运行。该系统还应包括航空利害攸关方之间(例如政府、业界以及适当情况下民用执法和军用部门之间)的适当合作和信息共享机制。

3.3 通过采用“按设计安保”做法，确保民用航空业实现自强

在民用航空领域采用按设计安保做法要求在系统构想之初就考虑到系统设计程序中需要实现的安保目标，以及传统的运行和安全目标。“按设计”确保关键要素和过程的安保，将安保模式从被动转变为主动，并促进自我防护型民用航空系统的发展，从而使其能够发展并增强安保和复原力。

3.4 确保在民用航空内部并与相关非航空利害攸关方协调航空网络安保

为确保航空各学科对航空网络安保采取一致且互补的做法，民航系统必须通过协调航空网络安保的安全和安保方面，确保全面管理民用航空面临的网络风险。此外，航空网络安保的协调范围应扩大到民用航空以外的其他有关实体，如国家/区域/国际网络安保主管部门、执法部门、军事部门等。

---

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx。

[2] 国际民航组织 2020/114 号国家级信件。

4. 网络安保政策要素

本节就纳入附录 A 所载的网络安保政策范本中的要素提供指南。因此，建议与网络安保政策范本一并读取。

4.1. 治理和组织

4.1.1 各国应指定航空网络安保主管部门(AA/Cyber)，总体负责航空网络安保和网络复原力。

4.1.2 对于航空网络安保主管部门在各国民航组织结构中的位置，并无普遍适用的模式。这一决定将受到与国家航空和相关非航空机构实体和任务方面有关的若干因素的影响。但必须向航空网络安保主管部门提供所需要但资源和授权，使其能够执行任务，包括与非航空相关利害攸关方谈判和协调。

4.1.3 总体而言，指定航空网络安保主管部门应：

- 与国家网络安保主管部门协调，确定各主管部门应承担的作用和责任；
- 牵头制定航空网络安保法规；
- 明确界定国家民航主管部门内对不同民用航空领域的作用和责任；
- 通过国家安全和安保方案，协调界定由国家民航主管部门监督的民用航空实体的作用和责任；
- 界定民用航空网络安保文化的要素并监测其落实情况；
- 界定网络安保危机管理的法规、流程、要求和作用，包括测试要求和频率；和
- 与信息共享和事故征候调查等航空网络安保所涉的相关非航空利害攸关方协调处理贯穿各领域的航空网络安保问题。

4.2 风险管理

4.2.1 管理网络安保风险应利用航空安全和安保风险管理框架，以便对网络安保威胁和风险进行综合和准确的评估，并确保制定和执行有效的缓解措施，同时考虑到各项安全要求以及缓解措施对民用航空安全和连续性的影响。

4.2.2 应始终明确所有数据和系统的所有权。明确和维护所有权使问责制得以确立，并有助于从采用到处置环节对数据和系统的管理。因此，所有者应制定规则和流程，以纳入数据和系统的物理位置、访问权限、管理权限以及基于数据和系统分类的安保要求。这最终有助于由适当的人员充分使用数据和系统，制定和执行质量控制标准，并解决问题和冲突。

4.3 关键系统安保

4.3.1 应运用纵深防御原则来保护关键系统。纵深防御整合了人员、技术和作业能力，以在组织的多个层次和任务之间设置可变的障碍[3]。这是一种将一系列防御机制分层处理以保护关键系统、数据和信息的网络安保做法。这种有意制造冗余的多层面做法提高了系统整体的安保能力，应对了许多不同的攻击向量[4]。

---

[3] 美国国家标准技术研究所（NIST）特别出版物 800-53 第 5 版：https://doi.org/10.6028/NIST.SP.800-53r5。

[4] 纵深防御通常被称为“城堡方法”，因为这种防御体现了中世纪城堡的分层防御，要想攻入城堡，进攻方必须面对护城河、吊桥、城墙、塔楼等。

4.3.2　航空网络安保主管部门应确保民用航空实体确定并充分保护其关键系统，以及发展检测、应对和从网络事故征候中恢复的能力。

4.4　数据安保

4.4.1　应将关键数据的定期离线安全备份视为实现信息可用性和完整性的手段。但必须根据风险评估制定有力的备份政策，因为在网络攻击发生时所做的离线备份已经受到损害，因此不能用于恢复对关键信息的访问。

4.4.2　应将敏感数据加密视为实现信息机密性的手段。但必须根据风险评估界定使用加密技术的程序，在保密级别和操作性能要求之间取得适当的平衡，特别是对于飞行安全所需的“实时”数据以及考虑到管理数据所需资源。

4.4.3　应创建流程，确保在数据可用性和/或完整性受损时关键功能的连续性。

4.5　供应链安保

4.5.1　各实体应确保在航空系统的整个生命周期，从设计和开发到运行和维护，再到安全和安保处置，用于关键航空功能的软件和硬件均符合网络安保要求。

4.5.2　可以利用服务水平协议，纳入网络安保对硬件和软件的要求，以及在发现漏洞时进行更新、升级和修补的要求。

4.6　物理安保

4.6.1　与航空网络安保相关的物理安保控制实例主要包括：界定物理访问管理和控制政策，对拥有系统/数据库行政权限或能够访问敏感和/或关键数据的人员进行背景调查，对能够访问或能够修改关键系统的人员的职责分离和/或轮调提出建议等。

4.7　信息和通信技术(信通技术)安保

4.7.1　与航空网络安保有关的信通技术安保控制实例包括，除其他外，访问控制政策和应用最小特权原则、软件/硬件防火墙和网络安保、加密技术、组织密码政策、终端保护、网络监测和异常检测、网络隔离、设备管理等。

4.8　事故征候管理和关键功能的连续性

4.8.1　航空网络安保主管部门应界定网络事故征候管理、关键系统恢复和连续性的法规、流程、要求和作用。

4.8.2　应利用现有的危机管理和业务连续性计划，纳入应对网络事故征候并从中恢复的内容。

4.8.3　应定期测试应急响应和业务连续性计划，以期改进计划和应急响应人员的能力。测试应纳入所有相关的利害攸关方，并结合桌面演习(TTX)和现场测试。

4.9　网络安保文化

4.9.1　应在所有航空实体中推行网络安保文化。

4.9.2　网络安保文化应得到组织领导层的认可，并应纳入由所有人员实施的方案。

4.9.3　该方案应包括经常性网络安保教育(包括网络卫生做法的原则)、对最新威胁的认识、培训和测试(同时纳入到培训和现场模拟攻击)，以评估网络意识/卫生水平。

4.9.4　网络安保文化应纳入安全和安保文化要素，如自我报告、报告可疑行为/做法、公正文化等。

— — — — — — — —

附录 A

网络安保政策范本

1. 引言

1.1 本网络安保政策应成为进一步发展和落实航空网络安保的框架。此项政策应予以公布，分发给相关利害攸关方并定期审查。

1.2 应编写进一步的指导材料，支持落实本网络安保政策。

2. 范围

2.1 航空网络安保应处理民航系统的安保和复原力问题，并支持与相关非航空实体和部门的合作，包括酌情与国家网络安保部门、国家安保、执法和军事部门合作。

2.2 航空网络安保应在国家一级与航空安全、航空安保、关键基础设施保护、网络防御和军事部门进行协调。

2.3 航空网络安保应在国际一级与指定负责航空网络安保的同等外国主管部门进行协调。

3. 目标

3.1 本航空网络安保政策的总体目标，是确保民航系统的安保、复原力和自强，以防范网络威胁和风险，并确保与有关国家当局和实体就航空网络安保进行协调。

4. 治理和组织

4.1 根据[针对该指定的法规/立法参考]，[实体名称]应当是整体负责航空网络安保和网络复原力的航空网络安保主管部门（AA/Cyber）。

4.2 该航空网络安保主管部门应：

- 与国家网络安保主管部门合作，界定各主管部门应承担的民用航空网络安保作用和责任；
- 协调和促进航空网络安保法规的制定；
- 确定、协调和支持航空安全和航空安保主管部门，将航空网络安保要求的监督和质量控制等要素纳入本国国家安全方案（SSP）和国家民用航空安保方案（NCASP）；
- 界定、支持和监测所有民用航空利害攸关方执行网络安保文化方案的情况；
- 界定网络安保危机管理的法规、流程、要求和作用；和
- 与航空网络安保所涉的相关非航空利害攸关方协调处理贯穿各领域的航空网络安保问题。

5. 风险管理

5.1 网络安保应以情报为导向，以威胁为基础，致力于管理风险。

5.2 风险管理应成为整个系统生命周期中的组成部分。

5.3 应始终明确所有数据和系统的所有权。

6. **关键系统安保**

6.1 应通过风险管理流程明确关键功能、系统和基础设施。

6.2 应采用按设计安保做法并结合纵深防御原则保护关键系统。

6.3 应将关键系统的冗余视为实现系统安全的手段。

7. **数据安保**

7.1 应在存储和传输期间根据数据和信息的敏感度曲线对其进行保护。

8. **供应链安保**

8.1 软件/硬件供应链的端到端管理应成为航空网络安保管理的一部分。

8.2 在航空系统的整个生命周期关键航空功能中使用的软件和硬件均应符合网络安保要求。

9. **物理安保**

9.1 物理安保(包括人员安保)应成为航空网络安保管理的一部分。

9.2 物理安保应保护人员、基础设施、设施、设备、材料和文件不受非法干扰，并保护关键航空系统不受未经授权的物理访问。

9.3 物理安保应通过支持查明威胁行为者和/或对民用航空关键基础设施进行攻击的可能性，促进风险管理。

10. **信息和通信技术(ICT)安保**

10.1 信通技术安保应成为航空网络安保管理的一部分。

10.2 信通技术安保应界定并执行合理的安保措施，并促进网络事故征候管理、恢复和运营连续性流程。

10.3 信通技术安保应通过查明漏洞、攻击向量和监测航空网络安保威胁格局的演变，促进风险管理。

11. **事故征候管理和关键功能的连续性**

11.1 运行安全和关键功能的连续性应是推动事故征候管理流程的主要因素。

11.2 测试危机管理和恢复计划应成为事故征候管理的组成部分。

12. **网络安保文化**

12.1 教育、认识、培训和演习计划应成为航空网络安保管理的组成部分。

12.2 网络安保文化应与现行的安全和安保文化充分协调。

12.3 网络安保文化应得到强有力的内部信息共享做法的支持，并尽可能得到外部信息共享做法的支持。

— 完 —