



第十四次空中航行会议

2024 年 8 月 26 日至 9 月 6 日，加拿大，蒙特利尔

议程项目 4: 空中航行系统的超联通
4.2: 网络安全和信息系统的韧性

民航计算机事件安全响应小组（CSIRT）

（由哥伦比亚提交）

执行摘要

计算机事件安全响应小组（CSIRT）为各实体提供 IT 安全响应解决方案，使其能够在预测或应对网络事件时做出实时决策，立即采取行动并尽快恢复。大多数国家都有关键基础设施计算机事件安全响应小组，在国家当局的领导下处理网络安全事务。然而，国家航空运输部门往往缺乏这种设施。当务之急是要专门为民航建立一个计算机事件应急响应小组（CSIRT）。

民航部门有责任确保运行和乘客安全。这倚赖于一层用于关键信息和业务的技术基础设施，需要全天候监测以预见网络威胁。

因此，国际民航组织应建立一个参考框架，为各国建立民航 CSIRT 提供指导并制定程序。

民航的 CSIRT 应有适当的治理结构，并符合国际网络安全标准。它应支持各国利用有助于实现这一目标的工具、人员和程序，制定国际民航组织提出的民航网络安全战略。

有鉴于此，我们建议国际民航组织发布专门为民用航空建立 CSIRT 及相关程序的指导意见，汇集各国民用航空部门利害攸关方的人力和技术性网络安全资源。

行动：请会议建议国际民航组织制定指南和程序，以便所有成员国在本组织的领导下建立民航计算机事件安全响应小组并指定其职能。

¹ 西班牙文本由哥伦比亚提供。

1. 引言

1.1 国际民航组织网络安全战略认识到对信息技术系统的依赖性日益增加，确保信息的完好性、保密性和可用性对该部门的安全发展十分重要。民用航空面临的网络威胁不断演变，危及运行安全和连续性。威胁的动机可能是政治、金融、恐怖主义或其他目的。为了应对这种威胁，我们建立了一个以七大支柱为基础的参考框架：

- a) 国际合作；
- b) 治理；
- c) 有效的法律法规；
- d) 网络安全政策；
- e) 信息共享；
- f) 事件管理和应急规划；
- g) 能力建设和培训；和
- h) 网络安全文化

2. 讨论

2.1 民航部门及其利害关系方包括机场、通信、导航和监视（CNS）、空中交通管理（ATM）、无人驾驶飞机系统交通管理（UTM）和气象（MET）提供者、设备制造商和分销商、维修组织和航空公司，所有这些都通过信息和通信技术相互连接。这使得数据和信息的安全处理和管理变得更加复杂，对生命安全构成潜在风险。因此，利害关系方之间和主权国家之间应开展团队合作、协调和共享威胁情报。

2.2 主权国家在最具战略意义的层面上设有负责网络安全政策的机构和/或实体，其工作由计算机应急响应小组（CERTs）执行。在较低层面上，各部门的计算机事件应急响应小组（CSIRT）开展协调并采纳应对网络事件的规程，特别是在拥有关键基础设施的实体和/或部门中。民航就是这样一个部门，因此建立一个专门的 CSIRT 是合乎逻辑的。

2.3 有鉴于此，我们建议国际民航组织为各国建立民航 CSIRT 制定指南和程序，以实现提高民航网络复原力的共同目标。

3 结论

3.1 请会议同意以下建议：

建议 4.2/x — 关于建立民航计算机事件安全响应小组（CSIRT）和相关程序的指南

国际民航组织制定指南和程序，以便所有成员国在本组织的领导下建立民航计算机事件安全响应小组并指定其职能。

— 完 —