国 际 民 用 航 空 组 织

工 作 文 件

A40-WP/295
TE/119
1/8/19

大会 — 第 40 届会议

技术委员会

议程项目30：由技术委员会审议的其它问题

将国家网络安保管制措施适用于航空部门

（由新西兰提交）

执行摘要

本文件讨论了在当前各国所采用的网络安保管制措施并非具体针对航空部门这一背景下，国际民航组织航空网络安保框架的制定情况。该文件提议，国际民航组织应将工作重心放在制定强有力和商定一致的原则上，以便各国能够依照这些原则处理网络安保问题。

行动：请大会：

a) 注意到实施全球统一和过于规范的航空网络安保标准可能会与各国的国家网络安保框架发生冲突，并限制各国遵守国际民航组织标准和建议措施的能力；

b) 鼓励国际民航组织将重点放在拟定航空部门网络安保方面的原则性指南上，以协助各国将航空纳入国家框架，同时对ISO 27000系列等既定的信息安保标准加以考虑；和

c) 鼓励国际民航组织就信任框架的目的和适用提供指导。

战略目标：	本工作文件涉及战略目标：安保与简化手续，和安全。
财务影响：	不适用
参考文件：	AN-Conf/13-WP/270号文件：航空网络安保中的“各系统组成的系统”的概念（28/09/2018）

1. 引言

1.1 随着技术的不断进步和航空系统复杂性的不断提高，全球航空系统的安全和安保越来越依赖于采取有效的网络安保管制措施。

1.2 各个不同的部门对有效的网络安保管制措施有普遍需求，决不是只有航空部门才有此需求。如果没有有效的网络安保，各组织将难以在提供数字产品和服务的同时留住客户和利害攸关方对它们信任和信心。

1.3 各国应发挥作用，确保国家重要组织和部门在网络安保方面始终保持高水平。针对不同的威胁、能力和国家安全利益，各国采取的做法将各不相同。

1.4 尽管各组织实施的安全管制措施的类型通常会根据它们的需要和能力，以及它们所在部门的需要和能力进行调整，但国家安全利益会压倒一切。一国的国家利益总是优先于单个部门或组织的利益。

1.5 全球航空高度依赖于在航空界成员之间，包括在国家之间安全可靠地进行信息的数字化传输。在第十三次空中航行会议上提交的 AN-Conf/13-WP/270 号文件介绍了一个概念，即针对网络安保采取一种“由各系统构成的系统”做法。该做法认识到：整个航空系统由多个子系统组成，而这些子系统由一系列利害攸关方运营；需要对这些子系统做通盘考虑，以营造一个安保的运营环境。

1.6 为了能够在利害攸关方之间建立可信的通信联系，国际民航组织拟定了一个信任框架。该框架涵盖以下原则：

1.6.1 通过建立一个共同的信任框架和架构，在全球范围内实现无缝和高效的信息传递服务，确保所有利害攸关方之间的互操作性。

1.6.2 通过使用可限制威胁面的设计概念，最大限度地提高通信的自我恢复能力。这涉及到网络和应用程序的分区、基础设施保护措施的分层，以及对参与进来的系统的数量进行限制。

1.6.3 加强身份识别、身份验证、授权、完好性和机密性。

1.7 虽然信任框架的概念有其价值，但其目的和潜在应用并不明确。在该框架的进一步拟定过程中，将需要认真考虑各国的国家安保利益，以确保框架的作用得以明确界定。

2. 讨论

2.1 一国的国家利益限制着各个部门和组织所能实施的网络安保框架的性质。如果国家拟定了信息安保方面的监管要求和标准，它们将优先于某个具体部门和组织的标准。

2.2 因此，一国遵守国际民航组织关于航空网络安保的规范性标准和建议措施的能力可能会受到本国国家安保框架的限制。这种受限制的程度在各国之间会存在很大差异，并且根据标准和建议措施本身所具约束力的大小而存在很大差异。

2.3 同样，如果某一做法高度规范化和高度标准化，则不太可能用于对技术和威胁环境都在快速演变的某一地区进行监管。过于规范化的全球性要求可能会阻碍一国应对变化的能力，可能不能同等地适用于不同类型的运行。

2.4 尽管各国网络安保需求不同，以及在实施高度规范性国际要求方面面临着问题，但仍有必要拟定一套统一和商定一致的原则，对利害攸关方之间的信息安全传输进行管理。

2.5 为了支持这些原则的实施，国际民航组织应编写指导材料，重点是协助各国支持航空网络安保，将其作为国家框架的一个组成部分。要实现这一点，采取基于绩效或原则的做法可能最有效。

2.6 通过采用一种基于原则的做法，各国可对国际民航组织的指导材料进行调整，使全球信任框架能够在符合国家要求的情况下得到实施。现有的基于原则的信息安保标准，如 ISO 27000 系列，可为此种指导材料的编写提供依据。最好涉及如下四个关键方面：

2.6.1 **治理**：在某一组织的高级领导层一级推动网络安保工作，以保护该组织最重要的数字资产。董事会和行政人员对任何网络事件的后果，包括对利害攸关方和客户信心所遭受的影响担负最终责任。

2.6.2 **投资**：投资于网络安保，使风险最小化且回报最大化。在管理层一级就组织的风险偏好达成一致及对关键资产予以查明乃是确保投资方向正确和取得适当均衡的关键性第一步。

2.6.3 **准备就绪**：让组织做好准备，以便发现网络安保事件、对事件做出回应，以及从中恢复过来。这是一个组织将于“何时”经历网络安保事件的问题，而非组织“是否”会经历网络安保事件的问题。未雨绸缪能让组织从事件中迅速有效地恢复过来，从而降低整体网络安保风险。

2.6.4 **供应链**：始终监督和认识到某一组织供应链中的网络安保风险。此方面对航空部门尤其重要，因为在提供设备和服务时所涉及的供应链往往非常长。这包括系统设计的技术组成部分，以及过程设计的人的因素方面。

2.7 以既定的信息安保标准为依据，制定完善的基于绩效的指导材料，对航空部门内各个组织是有价值的，并将鼓励采取一种涵盖有效网络安保管制措施其关键要素的一致性做法。

2.8 制定此种指导材料还应考虑需要在哪些方面实施某些最低限度的管制措施，以及在对不同国家所适用的框架做出考虑的情况下，应如何实施这些管制措施。

2.9 国际民航组织信任框架的制定可提供一个机会，用于拟定在利害攸关方之间进行信息互换的规程，但需要进一步澄清该框架的目的和适用情况。

2.10 信任框架的拟定应与利害攸关方实施的网络安保框架一起考虑。数据交换的安全性只可达到数据源的安全性水平，并且这取决于组织和国家采用的有效管制措施。

— 完 —