国 际 民 用 航 空 组 织

工 作 文 件

A41-WP/488[1]
EX/235
2/8/22

大会 — 第41届会议

议程项目15：审计计划 — 持续监测做法

加强各普遍安保审计计划持续监测做法小组以评估和实施附件17关于网络安保的要求

（由委内瑞拉（玻利瓦尔共和国）提交，并得到多民族玻利维亚国、哥伦比亚、哥斯达黎加、巴拿马、秘鲁和乌拉圭[2]的支持）

执行摘要

根据普遍安保审计计划（USAP），各国当前具备了指导准则，得以对国家航空安保监督系统进行一次总体的绩效评估，从而能够运用共同的航空安保原则，制定改进该系统的建议。这样一次评估是由一组审计员进行，他们将确保这些活动涵盖的范围除了附件 17（《航空安保》）的标准所作规定和得到的遵守程度之外，还包括航空安保监督系统的各个关键要素。 附件 17 具体规定了如何制定和实施措施来保护信息和通信技术系统以及用于民用航空目的的关键数据。有鉴于此，需要加强各审计小组，为此制定指导或培训材料，使这些小组能够评估和实施附件 17 所载网络安保要求。

行动：请大会：

a) 注意到本工作文件提供的信息； 和

b) 要求理事会制定工具或培训材料，为普遍安保审计计划审计小组提供网络安保方面的充分指导和培训，使指派的小组能够在专门化的民用航空网络安保层面对规程问题（PQ）进行客观的技术评估。

战略目标：	本工作文件涉及以下战略目标：安保与简化手续。
财务影响：	我们提议使用本三年期经常预算可以提供的资源和/或预算外捐款开展本文件所述各项活动。
参考文件：	附件17的建议措施4.9.1和普遍安保审计计划持续监测做法规程

[1] 西班牙文本由委内瑞拉（玻利瓦尔共和国）提供。
[2] 南美（SAM）地区和拉丁美洲民航委员会（LACAC）的成员国。

1. 引言

1.1 普遍安保审计计划（USAP）为各国提供指导准则，使其得以对国家航空安保监督系统进行一次总体的绩效评估，从而能够运用共同的航空安保原则，制定改进该系统的建议。根据普遍安保审计计划持续监测做法（USAP-CMA）规程，目前有一些特定的规程问题（1345、1350、1360 和 3278），涉及制定和实施措施，保护信息和通信技术系统以及用于民用航空目的的关键数据的工作在一般性方面或基本方面的内容。

1.2 这样的评估由一组普遍安保审计计划审计员进行，他们确保这些活动涵盖航空安保监督系统的各个关键要素以及附件 17 （《航空安保》）标准所做规定和得到的遵守程度。附件 17 包括每个国家都做出的以下承诺：分配责任；制定国家标准，用于通过实施保护性措施来保护与航空运行相关的系统；确定关键系统；进行持续监测；确保发现、分析和应对网络攻击；评估国家根据风险评估开展的质量控制活动。

2. 分析

2.1 鉴于根据 USAP-CMA 所开展活动的重要性，必须在网络安全方面确保向普遍安保审计计划的审计小组提供指导材料，使其能够对各国为确定和保护关键信息技术和通信系统，使其免受可能损害民用航空系统安全、完整性或运行的任何干扰而制定和实施的国际标准、战略和最佳做法进行客观的技术性评估。

2.2 我们目前掌握全球一级的参考框架和现有做法，使各种组织能够高效管理和降低网络安保风险。一些例子包括：ISO/IEC-2700 系列标准，其目的是确立信息安保管理、持续改进和风险缓解各个方面的良好做法；信息及相关技术控制目标（COBIT）指南； MAGERIT 信息系统风险分析和管理方法；以及其他国际标准、准则和最佳做法。

2.3 上述参考文件代表了网络安保合作和全球一体化的重大进展，提供了适用于所有类型的关键基础设施的共同行动方针和基准。这些基准特别涉及行业标准、指导准则和做法，使网络安保的实施和评估成为可能，不仅在组织和文件层面如此，而且在运营和实施方面也是如此。

2.4 考虑到这一点，我们提议制定标准化指导材料，从而能够利用行业最佳做法和方法以及各国经验来创建一个参考框架，以实现做法的统一。这个框架不一定是静态的文件，而是指导材料，使普遍安保审计计划审计员们能够根据规程问题 1345、1350、1355、1360 和 3278 中显示的每个国家的具体情况和需要，对标准得到的遵守程度进行技术性和客观的评估。

2.5 本工作文件的附录载有为各个知识领域和指导材料建议的内容模型。这项建议所根据的标准来自具有国际性重要基础设施的组织所采用的各种信息安保管理、持续改进和风险缓解标准、准则和现有做法。附录强调了以下内容：

a) 为评估各国实施的网络安保措施而可能必需的各种知识领域和经验（以规程问题为依据）；和

b) 为起草案文或指导材料所建议的内容，目的是使普遍安保审计计划的审计小组能够评估和实施附件 17 规定的网络安保要求。

3. 结论

3.1 获指派实施普遍安保审计计划持续监测做法的审计小组必须拥有必要的工具和知识，以准确、客观地评估各国按照国际民航组织附件 17（《航空安保》）的标准和建议措施提出的要求，遵守规定，为民用航空网络安保设计、制定和实施保护任务的情况。

— — — — — — — —

附录

为知识领域和指导材料建议的内容

a) 为评估各国实施的网络安保措施所必需的知识领域和经验

了解资产管理和关键流程的程序和技术；识别和评估与航空相关的技术资产或信息；信息安保政策、程序和措施；风险和事故征候管理；能够缓解网络安保所发现问题的管理控制措施或保障措施；取证、网络、代码、漏洞和物理审计、网络分析及其他。

通过进行测试来评估保护措施的技术能力，例如：资产的收集、分类和识别；服务扫描；漏洞分析和验证；当电力系统出现故障时对供电系统、设备、依赖供电的资源或系统进行运行测试检查；对信息系统和 IT 平台管理设备进行测试；对硬件、操作和基础设施软件和/或软件应用程序进行测试；对 IT 平台进行性能测试（在供电全部中断的情况下）；互联网备份服务测试（主通道断开、副通道连接检查、负载均衡等）；信息恢复测试等。

b) 为能够评估和实施附件 17 中的网络安保要求而建议的用于起草案文或指导材料的内容

1. 以下指南：民用航空业与航空公司有关的通用关键流程（旅客、行李、货物、地面协助、飞行调度、航空器维修等方面的管理）；机场关键流程（机场安保、运营和机场基础设施、管理和机场紧急情况等）；航空运输管理的关键流程（语音通信、航空通信和雷达数据、空中航行等）。

2. 航空业的标准化风险评估方法，包括确定背景、政策和责任；明确运营流程；查明和评估资产；确定脆弱性；确定威胁、其发生概率和估计影响（后果）。

3. 控制措施或保障措施指南，包括：网络硬件管理；授权和未授权软件的管理；移动设备、笔记本电脑、台式电脑、服务器的基本配置；持续的漏洞识别和修复流程；管理权限（网络/应用程序）的使用和配置情况识别、预防和纠正流程和工具；审计结果的维护、监测和分析；电子邮件和导航器保护程序；网络设备中的端口、协议和服务的管理；基于适当方法和工具的关键信息备份和恢复测试程序；网络装置（防火墙、路由器和交换机）的安保配置程序；外围防御；旨在防止信息丢失、减轻事件影响并确保敏感信息的机密性和完整性的数据保护程序和工具；事件管理和应对程序以及其他控制措施。

— 完 —