第 11 次航行会议

2003 年 9 月 22 日至 10 月 3 日，蒙特利尔

议程项目 2： 空中交通管理（ATM）的安全和保安
2.5：ATM 基础结构的安全和保安

法国空中航行办公室的运行网络计算机保安方法

（由法国提交）

摘要

现在，计算机系统已在空中航行中占据主要位置，且其安全和保安对于完成空中航行服务的任务至关重要。

本文件旨在介绍法国空中航行办公室为处理其运行信息系统的计算机保安问题所采用的方法。

会议的行动在第 5 段。

1. 背景：法国空中航行办公室的计算机保安和安全问题

1.1 维持一个信息系统的安全，可以用保障其可供使用性、完好性和保密性来界定。保安可被视为信息系统安全性的一个分支，则专门旨在保护信息系统的安全免遭恶意攻击。

现在，计算机系统已在空中航行中占据主要位置，因此信息系统的安全和保安对于完成空中航行服务的任务至关重要。

直到几年前，空中航行信息系统还是封闭的，与外界只有很少或几乎没有任何联系。那时它不易遭受保安威胁，仅仅是因为从外界的任何地方都难以通过计算机进入信息系统。在这种情况下，**保安**可以被局限为保护信息系统免遭实际进入。

1.2 然而，这些年以来，我们已经看到，随着信息系统对于空中航行重要性的提升，系统也逐步变得更为复杂，而且正在演变成一个与空中航行服务控制之外的其他系统和网络的互联日益紧密的系统。这种互联是必要的，因为需要与空中航行服务的伙伴（欧洲伙伴，航空公司等）相互联系和交换数据。同时，“专有”技术正在逐步让位给标准技术，诸如用于网络的 IP（互联网议定书）或用于运作系统的 UNIX 等。

所有这些因素都使得信息系统更为敏感，并增大了遭受外部威胁的风险。因此，恶意肇事者对信息系统进行保安方面侵害的风险大为增加。

1.3 法国空中航行办公室因而清楚地意识到，必须对维护其信息系统的保安和安全，特别是保护其免遭可能的外部威胁予以更多的关注。

2. 问题的处理

2.1 为了能将信息系统的风险降低到可接受的程度，必须明确能补救信息系统脆弱性的技术、组织和程序方面的保护措施。这样的措施必须体现以下规则：

— 完全彻底地解决问题；

— 明确统一的保护措施；

— 明确适用的、为人们所认同的和实际采用的保护措施。

2.1.1 完全彻底地解决问题，意味着涵盖可能会对保安有影响的所有方面，包括计算机系统与外界的互联，其内部互联（网址之间），计算机设备的使用、运行和维护，技术和功能上的改变，人力资源的组织和责任，以及保安事故征候或事故的管理。

为了做到完全彻底，覆盖面还必须考虑信息系统中具有“安全要求”，或对其所进行保安方面的侵害可能会影响空中航行任务执行的所有因素。

2.1.2 计算机系统以内的保护措施必须是统一的。实际上，计算机系统有效保护的水平就是其最薄弱环节的水平。因此，如果在系统的一个部分施加繁冗复杂和花费昂贵的保护措施，而另一个同样敏感的部分却得不到多少保护，那么这样的做法是徒劳无益的。

2.1.3 保护措施必须是适用的，且必须考虑到情况的限制条件和具体性质。在起草保安规则时，所使用的技术、运行上的保安限制、使用者和操作者的习惯和做法等都必须考虑在内。最后，为了使这些规则实际得到采用，最为重要的是规则能为计算机系统的操作者和使用者认同。他们必须熟悉这些规则，且这些规则在系统运行与使用中应和已经存在的规则同样适用。

2.2 考虑到所有这些因素，法国已开始形成一套高级别的计算机保安总体政策。这一项目称之为PSINA（空中航行信息保安政策）的项目，其目的在于明确计算机保安的总体规则，适用于所有作为空中交通管制信息系统（SICTA）一部分的空中航行“运行”系统。

将这一总体保安政策制成文件时，应包含以下章节：

— PSINA 的目标和限制范围：用于信息系统的定义，采用的原则，处置的威胁和 PSINA 相对于其他现行规则的地位；

— 信息系统组成部分的分类：为信息系统的功能和物质组成部分规定的 4 个级别的敏感度，以及对不同级别的组成部分进行分类的标准。分类按三个方面进行：可供使用性、完好性和保密性；

— 用户进入信息系统：民航总局聘用外部职员时，在保安许可、授权、验证、行动的可追踪性和使用方面的规则；

— 实际保护：保护敏感信息媒介（可移动或携带的媒介等）、保护和实际放置计算机系统的规则；

— 信息系统的维护和管理：维修人员的保安许可、验证、外部维修技术人员的聘用、系统维护和管理操作的可追踪性方面的规则；

— 信息系统内部的系统互联和数据交换：采用“可信领域”确定统一保安参数和为在使用私人或公共网络进行内部互联的规则；

— 与外部实体的互联和数据交换：从外部进入信息系统和从信息系统进入外部实体的规则，使用公共或私人网络与外部互联的规则，信息系统和外部实体之间发出和接收计算机数据的规则；

— 信息系统的演变：信息系统每次改进后对其组成部分分类和安全水平所做的重新评估；安装新组成部分或撤消旧组成部分的规则；

— 保安事故征候和事故：保安事故征候或事故的定义，事故征候的分类和检测，检测到保安事故征候后采取的行动，就保安事故征候和事故进行内部和外部联络的规则；对民航总部内外恶意肇事者的惩罚措施与处理原则的定义。

— 涉及信息系统保安的人力资源的组织：使用者对于保安/安全问题的认识和决策者对于保安问题的认识，“保安”官员的授权，保安行政管理和维护规则，等。

2.3 为了确保根据这一保安政策制订的规则能予适用，且信息系统所涉人员能迅速掌握这些规则，成立了一个工作组，任务是草拟政策提案。工作组由空中航行服务各运行部门的代表组成。此外，为了保证 PSINA 得到各操作者和使用者的有力认同，它将由空中航行办公室主持的监督委员会通过，以此来保证其权威性。

2.4 根据 PSINA 拟定的保安规则举例如下。

— 与外部系统进行任何互联，须经保安官员根据具体提及以前所做风险研究结果的保安档案对其作出正式批准。

— 与外部进行任何互联，必须在技术上核实。这尤其是为了保证在某一具体时刻，只有经批准进行此种互联的服务才能进入，且只有经批准的联络人（用户或系统）才能使用系统，等等。此外，所进行的核实还必须可以保证，只有经批准的功能性服务所严格要求的技术服务（如网络议定书）才能在互联中使用。

— 对于信息系统中最为敏感的要素，严禁使用公共网络（RTC，互联网等）建立任何互联。

3. 所采用方法的强化战略

3.1 由于 PSINA 项目的规模，并为了逐步应对其所有方面，在其目标中确定了一些优先事项。

第一项目标是保障空中航行信息系统的界线，以对付外部风险。这一点可以通过确定必须在信息系统边界强化保安功能和规则来实现。

一旦保障了这一界线，然后就可以处理内部保安。对内部风险的应对更难以确定，所需要的措施也复杂得多，因为不可能“锁住”整个系统；实际上，信息系统必须保持能够使用而且高效运行，因此不可能采用对付外部风险那样的激进和相对简单的保护措施。这就是为什么决定在首先处理了外部风险之后就转向这一事项的主要原因之一。

3.2 在整个目标的排序中，最终目标是能够提供“根深蒂固”的信息系统保安，用管制和保安技术对网络和网络互联进行边界防御，采用了保安技术的内部防御机制，重点放在内部网络和系统本身。

4. 结论

4.1 法国目前正在为确定其初步的计算机保安政策而继续努力。工作组已经起草了拟定前几个章节的提案，这是这一政策的基石（政策目标和限制范围，对信息系统组成部分进行分类的规则），工作组在继续起草关于与外部实体互联的规则。这第一项提案不久将呈交监督委员会。

4.2 一旦这前几个章节得到关于人力资源的组织和计算机保安的章节的补充，将可在法国空中航行办公室正式实施初步的空中航行计算机保安政策。

4.3 这是一项长期的任务，需要进行持续的努力，以最终制定与其目标相匹配的全面的保安政策。

5. 会议的行动

5.1 请会议：

a) 考虑威胁空中航行计算机系统的风险；

b) 拟定标准和建议措施（SARPs）以保障计算机系统的保安；和

c) 请一组专家制作一套普遍的指南，协助各国实施其安全和保安政策，比如采用检查单的形式，表明安全和保安政策触及的要点和问题，以及用以保障计算机系统保安的手段。

—完—