联合国 A/68/7/Add.11

大 会

Distr.: General
4 December 2013
Chinese
Original: English

第六十八届会议

议程项目 134

2014-2015 两年期拟议方案预算

关于加强全秘书处信息和系统安全的建议执行进展情况

行政和预算问题咨询委员会关于 2014-2015 两年期拟议方案预算的第八次报告

一. 导言

1. 行政和预算问题咨询委员会审议了秘书长依照大会第 67/254 号决议提交的关于加强全秘书处信息和系统安全的建议执行进展情况的报告(A/68/552)。大会在该决议中请秘书长在 2014-2015 两年期拟议方案预算中介绍处理信息安全问题各项行动的最新执行情况。在审议上述报告期间，行预咨委会会见了秘书长的代表，他们提供了补充信息和说明，行预咨委会最后于 2013 年 10 月 20 日收到了书面答复。

2. 行预咨委会回顾，在对秘书处信息和通信技术事务处理情况、包括信息和通信技术厅的第一次审查(A/67/651)中，审计委员会称联合国不具备足够安全的信息环境，并为解决薄弱环节提出一系列建议。秘书长在关于这些建议执行情况的报告(A/67/651/Add.1)中指出，秘书处正在拟定包括 10 项措施的行动计划，以采取短期措施处理最紧急的缺陷，并确定信息安全问题的可持续中长期战略。这 10 项措施主要涉及三个领域：(a) 预防性控制；(b) 提高侦测和响应能力；(c) 治理、风险与合规问题。

3. 秘书长的报告提供的资料述及信通技术的现状、执行加强信息安全行动计划的初步措施以及在这方面还需要采取哪些行动。秘书长指出，将在大会第六十九届会议上在信息和通信技术综合战略框架下提出全面的信息安全战略(包括网站和外地特派团)。

二. 迄今完成的活动

4. 秘书长的报告第 10 和 11 段提供的资料述及为执行行动计划而开展的活动，包括：(a) 加强预防性控制，包括限制行政特权，按当前安全要求重新配置服务器，购置更多电子邮件和互联网流动过滤系统，审查防火墙基础设施并以更先进技术取代之，购置基于计算机的培训课程以提高秘书处所有工作人员对信息安全的意识；(b) 在已经展开的查明执行“团结”项目后将继续运行的所有应用软程件序的工作中，开始评估目前在运行的所有软件应用程序构成的安全风险；(c) 已为总部(纽约和新泽西)的主用数据中心和备用数据中心以及巴伦西亚联合国支助基地和意大利布林迪西联合国后勤基地的企业数据中心购置管理服务，以部署和持续运行入侵检测系统，并合并整个秘书处现有的网络情报来源。

5. 行预咨委会询问购置安装电子邮件和互联网(网站)过滤系统的状况后获悉，已经在现有的系统合同下购置了先进的互联网流动过滤系统，目前正在开展实施该系统所需的活动，包括调整支撑基础设施和修订现行的互联网过滤政策。购置先进的电子邮件流动过滤系统需要一个竞争性采购过程；这项工作已于 2013 年 3 约启动，目前仍在进行之中。在完成采购过程之前，已经签了一项短期租赁合同作为临时安排，从 2013 年 11 月底生效。**行预咨委会建议，请秘书长在下一次关于这个问题的报告中，保证以成本效益尽可能最高的方式，采购为实施信息安全行动计划而购置的产品和服务**。

6. 关于秘书长的报告第 10(a)段提及的基于计算机的培训课程，行预咨委会获悉，已经签了一项费用为 35 826 欧元的合作，用于编制基于计算机的信息安全意识培训课程，涵盖范围为全联合国系统信息安全专题组确定的“核心内容”。这项课程对全体工作人员将是必修的，预计将于 2014 年早些时候在秘书长公共电子学习平台(Inspira)上推出。**行预咨委会鼓励秘书长继续推动全系统的合作，寻求一切可选办法推进联合国系统各组织之间扩大合作，并交流处理信息安全问题的解决办法**。

7. 秘书长指出，除根据行动计划采取措施外，本组织还在对其全球信通技术业务启动重大改革，以加强使用控制和减少受到入侵的脆弱性，从而支持实施企业资源规划“团结”项目。例如，这包括实施新的全球广域网，全部企业系统采用标准接入层(思杰)，向巴伦西亚和布林迪西企业数据中心转移软件应用程序。**行预咨委会建议，大会请秘书长尽可能加速向企业数据中心转移应用程序，并在上述关于新信通技术战略的报告中全面报告进展情况**。

8. 秘书长又指出，2013 年 7 月，信息和通信厅决定聘请对秘书处信息安全状况进行独立评估，主要重点是总部的基础设施(A/68/552，第 8 段)。他讲到，评估证实和补充了内部审查结果，并显示了下列等问题：(a) 联合国没有设定足够的信息安全控制措施，不仅信息和通信基础设施的传统构成部分如此，而且传统上

没有数字化控制的建筑物管理系统、出入控制和监测解决方案、电话技术及视频会议系统和视听设备也是这样；(b) 外勤支助部需要新的软件工具取得入侵监测和过滤能力，同时将防火墙升级，以增强总部和外地的安全环境；(c) 需要密切审视外部托管的网站，同时审查安全控制措施并为秘书处各部门重新设计网站提供协助，以防范入侵或污损(同上，第 13-15 段)。

9. 秘书长还指出，由于对相互连通性的需求不断增加和秘书处信通技术系统的相互依存，任何地方的攻击或入侵都可导致所有地方受损；为执行该行动计划而在总部采取的措施需要在其他工作地点实施，并辅以本组织监测能力的大幅度增强(A/68/552，第 18 段)。此外，本组织信通技术网络各自为政的情况显然使确保安全变得更加困难和昂贵。秘书长讲到，从速将其数据中心迁往巴伦西亚和布林迪西，以更快地部署安全和监测措施并减少费用；消除各自为政的状态将是上述新信通技术战略的一个支柱(同上，第 20 段)。

10. **行预咨委会注意到，在实施行动计划解决信息安全方面取得了进展，秘书处打算减少各自为政的状态，并减少部署安全和监测措施的费用。行预咨委会重申在其前一次关于信息安全状况的报告中表达的意见，对拖延这么久才处理这个问题仍感到关切(A/67/770，第 68 段)。**

11. **另外，鉴于联合国涉及全球范围，其信息系统具有覆盖广泛的性质，行预咨委会认为，还需要保护本组织的通信和数据不受到大规模监视、拦截和收集；行预咨委会建议，大会请秘书长在下一次报告中提出确保这种保护的可能备选办法。**

治理、风险与合规问题

12. 在治理、风险与合规方面，秘书长指出，采取的行动包括：(a) 制定了一项信息安全政策指示，发给各部厅首长，作为本组织信息安全政策、程序和准则的总框架；(b) 正在制定 52 项信通技术政策和程序，以利增强系统性能、安全、工作成果完好性；(c) 设立了信息安全工作组，作为信通技术管理协调组的一部分，负责增强工作地点之间的沟通；(d) 正在建立内部合规职能部门，负责增强对内部政策和程序以及业内最佳做法的遵守；(e) 联合国系统行政首长协调理事会(首协会)的信息安全特别兴趣小组协同信息和通信技术厅制定了一套公共网站最低要求，这些要求已获得首协会信息技术网络的核可。此外，根据外勤支助部最近建立的安全政策框架，目前定期在巴伦西亚和布林迪西以及外地特派团对已部署信息系统、基础设施和其他信息资产进行安全评估(A/68/552，第 10(d)段)。

13. 行预咨委会要求提供关于秘书长的报告第 10(d)段所述安全政策框架的信息，特别是信息和通信技术厅如何就信息安全事项与外勤支助部合作，包括协调机制及其各自的作用与职责分工。行预咨委会获悉，上述框架对总部的外勤支助

部和外地特派团都适用。外勤支助部还制定了专门的外地特派团安全政策框架，以应对外地的业务要求以及具体的环境和风险状况。另外，信息和通信技术厅通过与外勤部不断的联络和协调，确保面向外地的方针适当符合秘书处的全球标准、政策和建议。此外，信息和通信技术厅与外勤支助部就共同使用的系统经常进行协商和保持密切合作，并交流关于信息安全事故和脆弱性的信息/数据。

14. **行预咨委会注意到发布了全秘书处范围的统一安全指示。行预咨委会建议，大会请秘书长继续努力，确保通过关于信息安全的共同政策与程序，以保证本组织所有级别各尽其责。行预咨委会重申，秘书长还应采取及时的补救行动，解决在整个秘书处内有效颁布和执行统一信息安全政策可能遇到的任何障碍。**

15. **此外，考虑到秘书处称联合国任何地方受到攻击或入侵都可导致所有地方受损，以及需要在所有工作地点实施安全措施和监测系统，行预咨委会强调，对整个秘书处的信息和系统安全必须采取全机构范围统一的办法，以确保在此领域不发生工作重叠或重复开支。行预咨委会建议，大会请秘书长确保将在新信通技术战略框架下提出的中长期信息安全战略(见上文第3段)必须以共同政策和工具为基础，并以成本效益最高和尽可能有效的方式解决目前信息安全环境各自为政的状态。**

其他问题

16. 行预咨委会回顾，大会迄今已经核准了将瓦伦西亚的设施用作二级运行状态电信设施(见第63/262号和第66/264号决议)。**行预咨委会再次建议，大会请秘书长确保提交大会审议文件中使用一致的设施名称，反映其用于信通技术的目的(A/67/780/Add.10，第29-31段)。**

三. 所需资源

17. 行预咨委会询问后得到过去5年来大会核定的安全相关资源总额以及实际支出，以及2012-2013两年期间发生的信息安全支出细目，有关资料载于本报告附件二和附件三。行预咨委会注意到，信息安全相关支出几乎翻了两番，从2010-2011年的110万美元增至2012-2013年的近410万美元。

18. 经询问为解决将由“团结”项目取代的系统的安全问题所设想的投资数额，行预咨委会获悉，有些遗留系统的主机操作系统不再得到支持，面临很大风险，因为供应商没有提供更新，无法防范新发现的脆弱性。如果可能的话，这些系统需要转移到有支持的操作系统。对于无法转移的系统，拟增加监测活动，以便更及时地查明任何潜在破坏行为并限制其影响。**行预咨委会确认有必要确保操作系统的信息安全，以保护联合国的设施，但行预咨委会强调，对于将由“团结”项目取代、近期将退役的系统，投资应该尽可能保持在最低限度。**

2014-2015 年拟议所需资源

19. 下一个两年期间，秘书长提议除其他外：(a) 扩大入侵检测服务和过滤解决方案，以覆盖总部以外各办事处和各区域委员会；(b) 将防火墙基础设施升级；(c) 加强内部安全监测能力；(d) 部署一个脆弱性管理系统，以使本组织能够积极主动地查出具体薄弱环节并优先加以弥补；(e) 对总部的非传统基础设施要素和总部以外各办事处、各区域委员会以及位于巴伦西亚和布林迪西的企业数据中心的信通技术环境进行更多保护和检测控制。

20. 为执行上述措施，2014-2015 两年期拟议增加所需资源 3 440 700 美元，主要包括：(a) 其他工作人员费用(581 400 美元)，用于：1 个 P-4 安全工程师(一般临时人员)所需资源，该职位将提供与应用最近实施的入侵检测系统有关的更多技术专长；2 个 P-3 员额，履行恶意软件分析、模式创建和事件相关性方面的新职能，并在渗透测试、脆弱性评估、报告生成和网络应用安全测试协调方面扩大现有能力；(b) 工作人员差旅费(150 000 美元)，用于支付两名工作人员前往总部以外所有办事处、区域委员会和位于巴伦西亚及布林迪西的企业数据中心为期至少两周的费用；(c) 订约承办事务(1 325 000 美元)，用于：部署和持续运行入侵防范系统(800 000 美元)；脆弱性管理系统(25 000 美元)；高度专门化的知识专长，以视需要开展与持续执行秘书处信息安全战略有关的活动(500 000 美元)；(d) 家具和设备(1 325 000 美元)，用于：增强防火墙基础设施(1 000 000 美元)；持续监测能力(200 000 美元)；网络应用程序安全测试(125 000 美元)；(e) 一般业务费用(59 300 美元)。

21. 行预咨委会询问后获悉，2014-2015 年拟议方案预算第 29E 款下拟议的资源包括持续执行下列信息安全和风险管理任务所需的资源：(a) 制定和维持信息安全政策并监测各组织单位合规情况；(b) 为信通技术风险评估和减轻风险活动提供支持；(c) 在信息安全事件管理方面进行协调并提供协助；(d) 协调回应和遵守审计建议；(e) 处理所有接入综管系统、正式文件系统、远程接入综管系统及“核心”系统的请求，以及其他涉及安全登记的请求。关于现有的人员配置资源，行预咨委会还获悉，信息和通信技术厅安全和结构科信息安全和风险管理股由 1 名信息安全干事(P-4)、1 名信息安全干事(P-3)和 2 名信息安全助理(一般事务人员/其他职等)组成。还有 2 个相当于 P-4 职等的一般临时人员职位对这项能力构成补充，其中 1 个是合规干事，另 1 个是灾后恢复专家。此外，在其他大多数部厅，信息安全相关活动由同时还履行其他职责的工作人员和订约人开展。根据 2013 年初进行的一项调查，全秘书处共有相当于 12.5 个专业和一般事务职等专任员额的人力专门从事信通技术安全工作。

22. 行预咨委会回顾，大会第 67/254 号决议请秘书长在 2014-2015 两年期拟议方案预算中报告信息安全问题。**虽然秘书长已说明，拟议预算的部分依据是 2013 年 6 月进行的安全评估的结论，包括 2014 年扩大活动范围，以进一步加强总部**

以外各办事处、区域委员会和外地特派团的信息安全，但行预咨委会认为，秘书长报告中拟议的一些新的所需资源本来可以预计并列入2014-2015年拟议方案预算。而且，行预咨委会注意到，秘书长的提案涉及结构性和持续性资源需求，这些也会需要订正信息和通信技术厅2014-2015年核定工作方案（见A/67/6/Rev.1，方案25）。行预咨委会建议大会请秘书长确保今后尽一切努力，将持续性资源需求列入两年期方案预算，以便大会审议信息和通信技术厅所需资源总额。

23. 此外，鉴于需要以共同政策和工具为基础，在整个秘书处采取全机构范围统一的信息安全办法（见上文第14至15段），行预咨委会还建议大会请秘书长按照企业资源规划项目经费筹措所采用的费用分担安排（见第63/262号决议），分摊信息安全所需资源。

四. 结论和建议

24. 有待大会采取的行动载于秘书长的报告第30段。行预咨委会建议大会注意到秘书长的报告，但须考虑本报告中提出的意见和建议。行预咨委会还建议大会请秘书长：(a) 在2014-2015两年期拟议方案预算已编列的资源中安排临时人员所需追加经费和工作人员差旅费；(b) 在相关执行情况报告中报告订约承办事务（A/68/552，第27段）或家具和设备（同上，第29段）项下所需的任何额外支出。

附件一

已查明的安全问题和相关解决办法汇总表

问题	解决办法	说明
无法监测或发现因与手段先进的持续攻击有关的群体不断进行秘密或手段先进的活动而产生的网络流动。缺乏网络可见度	入侵检测服务	入侵检测服务将在网络中安置战略性网络工具，使所有网络流动具有可见度。该服务将使可疑活动引起“警报”，并实时捕捉网络流动。这些警报将被发送到一个支持公司，该公司将由专家团队梳理所收到的警报，并向联合国工作人员发出可采取行动的重要通知
使用通过电子邮件发送的高度定制化的恶意软件，使联合国资产(如工作站和台式计算机)不断遭到破坏。2013 年 9 个月来，这类攻击比 2012 年观察到的破坏增加了 76%	电子邮件高级过滤办法	定制化的恶意软件设法规避传统防毒办法的检测。高级过滤办法利用相关技术分析这类文件的行为，捕捉那些很可能会绕过现有解决办法的恶意软件
无法防范手段先进的持续攻击	下一代防火墙	目前，很多攻击都已设法绕过传统防火墙。下一代或现代防火墙保护应用程序采取额外步骤为本组织建立堡垒，这类程序已在纽约和两个企业数据中心使用。请求将这项能力扩展到所有地点，以确保统一保护联合国的网络。请求配置的工作人员对该系统的初始配置和运行至关重要
无法将多个系统的数据相互联系，以确定活动趋势，并参考系统的历史(记录)数据。缺乏可见度	持续监测(记录分析)	该系统收集多个系统的使用记录，以发现整个网络中的攻击趋势，并提供快速查询途径，以便在发现攻击时找到攻击历史。该系统对于建立所有安全系统的整体使用至关重要。请求配置的工作人员对该系统的初始配置和运行至关重要
缺乏资源，无法适当确定攻击源以及信息破坏行为导致的损害程度	恶意软件、法证和事件应对	请求配置的工作人员将提供快速检查能力，以查明破坏行为发生后可能丢失的信息或攻击机制，从而补充和增加提高联合国工作人员在该领域的技能
联合国信息系统在全球合规、更新和补丁方面的欠缺导致更大的脆弱性	脆弱性评估	通过使用自动化软件，持续进行监测及合规情况检查，以确保联合国所有系统“处于最新状态”，并确定仍然存在的脆弱性

附件二

2010 年以来信息和通信技术(信通技术)各年支出和总支出估计数

(美元)

	2010-2011 两年期			2012-2013 两年期		
	2010 年	2011 年	共计	2012 年	2013 年	共计
员额	318 000.00	318 000.00	636 000.00	719 600.00	773 450.00	1 493 050.00
咨询人		177 221.00	177 221.00	112 777.00		112 777.00
培训				436.67		436.67
ISO 27001 咨询人差旅				14 130.00	2 995.00	17 125.00
独立安全评估					60 000.00	60 000.00
ISO 27001 评估	24 000.00	33 025.49	57 025.49	38 170.90	1 545.00	39 715.90
专门服务器保护软件		64 276.10	64 276.10	7 122.15	7 122.15	14 244.30
端点保护软件	4 144.50	193 435.18	197 579.68	234 711.39	300 611.97	535 323.36
治理与合规软件				19 703.00		19 703.00
联合国总部电子邮件高级过滤办法					200 000.00	200 000.00
联合国总部防火墙				307 968.80	540 000.00	847 968.80
信通技术行动计划其他措施					715 158.00	715 158.00
共计	**346 144.50**	**785 957.77**	**1 132 102.27**	**1 454 619.91**	**2 600 882.12**	**4 055 502.03**

附件三

2012-2013 两年期间信息安全支出

(美元)

项目	名称	说明	价格	数量	共计
1.	**短期订购项目(低于 4 000 美元)**				
	网络安全人工测试软件	用于网络应用程序安全测试的综合平台。性能独特，具有多种供高级测试人员使用的专业化人工操作功能。低成本、高价值的工具	300	2	600
	基本脆弱性扫描软件	网络/服务器脆弱性自动化分析工具——低成本，允许使用多个服务器	3 900	1	3 900
	情报和分析工具	公开源码情报和法证应用程序，带有个案文件应用程序	760 + 200	1	960
	法证软件	领先的法证工具包，可用于台式计算机、服务器和移动装置。	2 999 + 599	1	3 598
	硬盘法证工具	用于从外部将先进技术警报系统硬盘与个人计算机联接，以便拷贝和(或)进行法证工作	75	2	150
				小计	**9 208**
2.	**询价项目(低于 4 000 美元)**				
	网站测试安全扫描工具	自动化网站安全测试/分析软件工具	5 950	1	5 950
	网站测试安全分析工具	自动化网站安全测试/分析软件工具	20 300	1	15 000
	防火墙管理软件	防火墙规则管理和跟踪软件	35 000	1	35 000
				小计	**55 950**
3.	**招标项目(30 000 至 200 000 美元)**				
	订约承办事务(防火墙专家)	聘用外部咨询人帮助重新设计网络和实施防火墙。11 月底、12 月初工作 1 个月时间	40 000	1	40 000
				小计	**40 000**
4.	**征求意见项目(进行中，情况各异)**				
	信息安全认识课程	制定提高信息安全认识的 HTML5 模块，在 Inspira 中使用	30 000	1	30 000
	电子邮件高级过滤系统	提供 FireEye 电子邮件管理安全服务工具和软件，包括电子邮件高级过滤专业服务	230 000	1	230 000
	Checkpoint Layer 7 防火墙	购买多个 Checkpoint Layer 7 防火墙和添加刀片	540 000	1	540 000
	管理安全服务	订立管理安全服务多年合同，包括网络监测所需的硬件、软件和外包安全专长	350 000	1	350 000
				小计	**1 150 000**
	总计				**1 255 158**