United Nations A/68/7/Add.11

General Assembly

Distr.: General
4 December 2013

Original: English

Sixty-eighth session
Agenda item 134
Proposed programme budget for the biennium 2014-2015

Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat

Twelfth report of the Advisory Committee on Administrative and Budgetary Questions on the proposed programme budget for the biennium 2014-2015

I. Introduction

1. The Advisory Committee on Administrative and Budgetary Questions has considered the report of the Secretary-General on progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat (A/68/552) submitted pursuant to General Assembly resolution 67/254, in which the Assembly requested the Secretary-General to provide an update on the status of implementation of the actions taken to address information security issues in the context of the proposed programme budget for the biennium 2014-2015. During its consideration of the above-mentioned report, the Committee met with the representatives of the Secretary-General who provided additional information and clarification, concluding with written responses received on 20 November 2013.

2. The Advisory Committee recalls that in its first audit of the handling of information and communications technology (ICT) affairs in the Secretariat, including the Office of Information and Communications Technology (A/67/651), the Board of Auditors stated that the United Nations did not have an adequately secure information environment and issued a series of recommendations for addressing the weaknesses identified. In his report on the implementation of those recommendations (A/67/651/Add.1), the Secretary-General indicated that the Secretariat was developing an action plan consisting of 10 initiatives to address the most urgent shortcomings, comprising short-term measures as well as the definition of a sustainable medium- and long-term strategy for information security. The 10 initiatives focused on three areas: (a) preventive controls; (b) improved incident detection and response capabilities; and (c) governance, risk and compliance issues.

3. The report of the Secretary-General provides information on the present situation with regard to ICT, the initial steps in the implementation of the action plan to strengthen information security and further action needed in this regard. The Secretary-General indicates that a comprehensive information security strategy, including websites and field missions, will be presented to the General Assembly in the context of the overall ICT strategy at the sixty-ninth session.

II. Activities completed to date

4. In paragraphs 10 and 11 of his report the Secretary-General provides information on the activities carried out to implement the action plan, which include: (a) strengthening of preventive controls by limiting administrative privileges, updating servers to current security levels, acquiring additional filtering systems for e-mail and Internet traffic, reviewing and replacing the firewall infrastructure with more advanced technology and acquiring a computer-based training course to raise awareness of information security among all staff across the Secretariat; (b) initiation of an assessment of the security risks posed by existing software applications in the context of the effort already under way to identify the applications that are to remain active after implementation of Umoja; and (c) acquisition of a managed service for the deployment and ongoing operation of intrusion detection systems for the primary and secondary data centres at Headquarters (New York and New Jersey) and at the enterprise data centres at the United Nations Support Base in Valencia, Spain, and at the United Nations Logistics Base in Brindisi, Italy, as well as consolidation of existing sources of cyberintelligence across the Secretariat.

5. Upon enquiry as to the status of the acquisition and installation of Internet (web) and e-mail filtering systems, the Advisory Committee was informed that an advanced Internet traffic filtering system had been acquired as part of an existing system contract and that the activities required for its implementation were under way, including modifications to the underlying infrastructure and an adjustment to the existing Internet filtering policy. The acquisition of the advanced e-mail traffic filtering system required a competitive procurement exercise which had been initiated in March 2013 and was still ongoing. Pending completion of the procurement process, a short-term leasing contract had been concluded as an interim arrangement with effect from the end of November 2013. **The Committee recommends that the Secretary-General be requested to provide, in his next report on this subject, assurances that the products and services acquired for the implementation of the information security action plan are procured in the most cost-effective manner possible.**

6. With regard to the computer-based training course referred to in paragraph 10 (a) of the report of the Secretary-General, the Advisory Committee was informed that a contract, at a cost of 35,826 euros, had been concluded for the development of a computer-based information security awareness training course to cover a common “core content” identified by the United Nations system-wide special interest group on information security. The course will be mandatory for all staff members and is expected to be rolled out in early 2014 on the common e-learning platform of the Secretariat (Inspira). **The Committee encourages the Secretary-General to continue to pursue system-wide collaboration and seek all options for further cooperation and sharing of solutions for information security among the organizations of the United Nations system.**

7. The Secretary-General indicates that, in addition to the measures implemented as part of the action plan, the Organization is introducing significant changes to its global ICT operations, enabling tighter access control and reducing vulnerability to intrusion, in order to support the implementation of Umoja, the enterprise resource planning project. These include, for instance, implementation of a new global wide-area network, the use of a standard access layer (Citrix) for all enterprise systems and the migration of software applications to the enterprise data centres in Valencia and Brindisi. **The Advisory Committee recommends that the General Assembly request the Secretary-General to accelerate, to the extent possible, the migration of applications to the enterprise data centres and to report comprehensively on progress achieved in the context of the above-mentioned report on the new ICT strategy.**

8. The Secretary-General further indicates that the Office of Information and Communications Technology decided, in July 2013, to obtain an independent assessment of the status of information security at the Secretariat, focused mainly on the infrastructure at Headquarters (A/68/552, para. 8). He states that the assessment validated and complemented internal findings and also revealed, inter alia, that: (a) the United Nations had insufficient information security controls in place, not only for traditional components of the information and communications infrastructure, but also with respect to systems that were not previously digitally controlled, such as building management systems, access control and monitoring solutions, telephony and videoconferencing systems and audiovisual devices; (b) the Department of Field Support is in need of new software tools to enable intrusion monitoring and filtering, along with upgraded firewalls, to enhance the security environment both at Headquarters and in the field; and (c) that there was a need to closely examine externally hosted websites, review security controls and provide assistance to the departments of the Secretariat in the area of website redesign in order to improve resistance against intrusion or defacement (ibid., paras. 13-15).

9. The Secretary-General also indicates that due to the increasing need for interconnectivity and the interdependence of the Secretariat ICT systems, an attack or intrusion anywhere could lead to a compromise everywhere, and that the measures taken to execute the action plan at Headquarters needed to be implemented at other duty stations and complemented by a significant enhancement of the monitoring capacity of the Organization (A/68/552, para. 18). In addition, the fragmented ICT network of the Organization made it more difficult and costly to ensure information security. The Secretary-General states that the strategy of the Organization is to expedite the transfer of its data centres to Valencia and Brindisi in order to deploy security and monitoring measures faster and to reduce costs, and that the elimination of fragmentation will be a central pillar of the above-mentioned new ICT strategy (ibid., para. 20).

10. **The Advisory Committee notes the progress made in the implementation of the action plan for addressing information security issues as well as the intention of the Secretariat to reduce fragmentation and costs in the deployment of security and monitoring measures. The Committee reiterates the views expressed in its previous report regarding the information security situation and remains concerned that this issue is only being addressed at such a late stage (A/67/770, para. 68).**

11. **Furthermore, given the global reach of the United Nations and the wide-ranging nature of its information systems, the Advisory Committee considers that there is also a need to protect the Organization against massive surveillance, interception and collection of communications and data, and recommends that the General Assembly request the Secretary-General to include in his next report, possible options for ensuring such protection.**

Governance, risk and compliance

12. In the area of governance, risk and compliance, the Secretary-General indicates that the actions taken included: (a) issuance of an information security policy directive to all heads of departments and offices as a general framework for the information security policies, procedures and guidelines of the Organization; (b) ongoing development of 52 ICT policies and procedures to help improve system performance, security and production integrity; (c) establishment of an information security working group as part of the ICT Management Coordination Group to increase the level of communication across duty stations; (d) ongoing development of an internal compliance function intended to increase adherence to internal policies and procedures and industry best practices; and (e) endorsement by the ICT network of the United Nations System Chief Executives Board for Coordination (CEB) of a minimum set of requirements for public websites developed by the Information Security Special Interest Group of the CEB in collaboration with the Office of Information and Communications Technology. In addition, under a recently established security policy framework by the Department of Field Support, security assessments of deployed information systems, infrastructure and other information assets were regularly conducted at Brindisi and Valencia and at field missions (A/68/552, para. 10 (d)).

13. The Advisory Committee requested further information on the security policy framework referred to in paragraph 10 (d) of the report of the Secretary-General, in particular, how the Office of Information and Communications Technology worked with the Department of Field Support on matters relating to information security, including coordination mechanisms and their respective division of roles and responsibilities. The Committee was informed that the aforementioned framework was applicable to both the Department of Field Support at Headquarters and field missions. The Department of Field Support had also developed a specific security policy framework for field missions to address the operational requirements and specific environment and risk profile in the field. In addition, through continued liaison and coordination with the Department, the Office of Information and Communications Technology ensured that field-specific guidelines were properly aligned to the global standards, policies and recommendations of the Secretariat. Furthermore, the Office of Information and Communications Technology and the Department of Field Support held regular consultations and maintained close collaboration with regard to commonly used systems and shared information/data on information security incidents and vulnerabilities.

14. **The Advisory Committee notes the issuance of a common, Secretariat-wide security directive. It recommends that the General Assembly request the Secretary-General to pursue his efforts and to ensure adoption of common policies and procedures regarding information security in a manner that assures accountability at all levels of the Organization. The Committee reiterates that the Secretary-General should also take prompt remedial action to address any**

hindrances that may arise to the effective promulgation and enforcement of common information security policies throughout the Secretariat.

15. **In addition, taking into account the statement of the Secretary-General that an attack or intrusion anywhere in the United Nations network could lead to a compromise everywhere, as well as the need to implement security measures and monitor systems at all duty stations, the Advisory Committee emphasizes the need for a common, enterprise-wide approach for information and systems security across the Secretariat which ensures that there is no duplication of efforts or dual spending in this area. The Committee recommends that the General Assembly request the Secretary-General to ensure that the medium- and long-term strategy for information security to be presented in the context of the new ICT strategy (see para. 3 above) be based on common policies and tools and address the current state of fragmentation of the information security environment in the most cost-effective and efficient manner possible.**

Other issues

16. The Advisory Committee recalls that to date, the General Assembly has approved the utilization of the facility at Valencia as a secondary active telecommunications facility and an enterprise data centre (see resolutions 63/262 and 66/264). **The Committee reiterates its recommendation that the General Assembly request the Secretary-General to ensure the application of a consistent designation of the facility throughout the documents submitted for consideration by the Assembly, reflecting its use for ICT purposes (A/67/780/Add.10, paras. 29-31).**

III. Resource requirements

17. Upon enquiry, the Advisory Committee was provided with the overall level of security-related resources approved by the General Assembly and actual expenditures over the past five years, as well as details on expenditures for information security incurred during the biennium 2012-2013, which are attached as annexes II and III, respectively, to the present report. The Committee notes that information security-related expenditures have almost quadrupled, from approximately $1.1 million in 2010-2011 to almost $4.1 million in 2012-2013.

18. Upon enquiry as to the level of investment envisaged to address security issues regarding the systems that are to be replaced by Umoja, the Advisory Committee was informed that some of the legacy systems were hosted on operating systems that were no longer supported and were at great risk, as no updates to protect against newly discovered vulnerabilities had been provided by vendors. Such systems needed to be migrated to a supported operating system, if possible. The systems that could not be migrated would benefit from the additional monitoring activities proposed to detect any potential breaches, in a more timely manner, and to limit their impact. **While recognizing the need to ensure information security of operational systems in order to protect United Nations facilities, the Committee stresses that new investments in systems that are to be replaced by Umoja and decommissioned in the near future should be kept to the minimum possible.**

Proposed resource requirements for 2014-2015

19. In the upcoming biennium the Secretary-General proposes, inter alia, to: (a) expand coverage of the intrusion detection service and filtering solutions to cover offices away from Headquarters and the regional commissions; (b) upgrade the firewall infrastructure; (c) enhance the internal security monitoring capacity; (d) deploy a vulnerability management system to enable the Organization to proactively identify specific weaknesses and prioritize their mitigation; and (e) conduct additional protective and detective controls for non-traditional infrastructure elements at Headquarters, as well as for the ICT environments at offices away from Headquarters, the regional commissions and the enterprise data centres in Valencia and Brindisi.

20. To implement the above measures, the proposed additional resource requirements for the biennium 2014-2015 amount to $3,440,700, mainly under: (a) other staff costs ($581,400) to cover the requirements for general temporary assistance for one P-4 security engineer to provide additional technical expertise associated with the application of the recently implemented intrusion detection system, and two P-3 posts to perform new functions of malware analysis, pattern creation and incident correlation, as well as to expand existing capabilities for penetration testing, vulnerability assessment, report generation and coordination of web application security testing; (b) travel of staff ($150,000) to cover the cost of travel of two staff members to all offices away from Headquarters, the regional commissions and the enterprise data centres in Valencia and Brindisi for a minimum two-week period; (c) contractual services ($1,325,000) to provide for the deployment and ongoing operation of intrusion detecting systems ($800,000), a vulnerability management system ($25,000); and highly specialized expertise to carry out, as needed, activities related to the ongoing implementation of the information security strategy of the Secretariat ($500,000); (d) furniture and equipment ($1,325,000) for enhancements to the firewall infrastructure ($1,000,000), continuous monitoring capabilities ($200,000) and web application security testing ($125,000); and (e) general operating expenses ($59,300).

21. Upon enquiry, the Advisory Committee was informed that the resources proposed under section 29E of the proposed programme budget for 2014-2015 included requirements for the continuation of the following information security and risk management tasks: (a) development and maintenance of the information security policy and monitoring of compliance across organizational units; (b) provision of support to ICT risk assessment and mitigation activities; (c) coordination and provision of assistance in managing information security incidents; (d) coordination of responses and compliance with audit recommendations; and (e) processing of all requests for access to IMIS, the Office Document System (ODS), remote access to IMIS and Nucleus and other security registration-related requests. With regard to existing staffing resources, the Committee was further informed that the Information Security and Risk Management Unit in the Security and Architecture Section of the Office of Information and Communications Technology comprised one Information Security Officer (P-4), one Information Security Officer (P-3) and two Information Security Assistants (General Service (Other level)). That capacity was complemented by two general temporary assistance positions equivalent to the P-4 level to provide for a Compliance Officer and a Disaster Recovery Specialist. Furthermore, in most other departments and offices, information security-related activities were carried out by staff and contractors, who performed other duties as

well. According to a survey conducted in early 2013, the equivalent of a total of 12.5 full-time posts at the Professional and General Service levels were dedicated to ICT security across the Secretariat.

22. The Advisory Committee recalls that, in its resolution 67/254, the General Assembly requested the Secretary-General to report on information security issues in the context of the proposed programme budget for the biennium 2014-2015. **Notwithstanding the statement of the Secretary-General that his proposals are based, in part, on the outcome of the security assessment conducted in June 2013, including the broadening of the scope of activities in 2014 to further strengthen information security at offices away from Headquarters, at the regional commissions and in field missions, the Committee is of the view that some of the new requirements proposed in the report of the Secretary-General could have been anticipated and included in the proposed programme budget for 2014-2015. Moreover, the Committee notes that the proposals of the Secretary-General concern requirements of a structural, ongoing nature, which will also require a revision of the approved programme of work of the Office of Information and Communications Technology for the period 2014-2015 (see A/67/6/Rev.1, Programme 25). The Committee recommends that the General Assembly request the Secretary-General to ensure that, in the future, every effort is made to include requirements of an ongoing nature in the biennial programme budget in order to facilitate its consideration of the overall requirements of the Office of Information and Communications Technology.**

23. **In addition, given the need for a common, enterprise-wide approach to information security across the Secretariat based on common policies and tools (see paras. 14 and 15 above), the Advisory Committee further recommends that the General Assembly request the Secretary-General to apportion the resource requirements for information security on the basis of the same cost-sharing arrangement applied for the financing of the enterprise resource planning project (see resolution 63/262).**

IV. Conclusions and recommendations

24. The action to be taken by the General Assembly is set out in paragraph 30 of the report of the Secretary-General. **Subject to its comments and recommendations in the present report, the Advisory Committee recommends that the General Assembly take note of the report of the Secretary-General. The Committee further recommends that the General Assembly request the Secretary-General to: (a) accommodate any additional requirements for temporary assistance and travel of staff from within the resources provided for in the proposed programme budget for the biennium 2014-2015; and (b) report in the relevant performance report on any additional expenditures required under contractual services (A/68/552, para. 27) or under furniture and equipment (ibid., para. 29).**

Annex I

Summary of identified security issues and related solutions

Issue	*Solution*	*Description*
Inability to monitor or discover network traffic generated from continued covert or advanced activities by groups associated with advanced persistent attacks. Lack of network visibility	Intrusion detection services	Intrusion detection services will provide for the strategic placement of network appliances within the network to provide visibility over all network traffic. The service will enable “alerts” of suspicious activities and capture of network traffic in real time. These alerts will be sent to a supporting company that will provide a team of experts to comb through resulting alerts and provide United Nations security staff with actionable critical notifications.
Continued compromise of United Nations assets such as workstations and desktops through the use of highly customized malicious software sent via e-mail. Such attacks have risen by 76 per cent over nine months in 2013 as opposed to observed compromises in 2012	Advanced e-mail filtering	Customized malicious software is designed to avoid detection by traditional anti-virus solutions. The advanced filtering solution employs techniques that analyse the behaviour of such files and catch malicious software that most likely would have bypassed existing solutions
Inability to protect against advanced persistent attacks	Next-generation firewalls	Currently, many attacks are now designed to bypass traditional firewalls. Application of next-generation or modern firewall protections, which take additional steps to bastion the Organization, have been applied in New York and at two enterprise data centres. The request is for expansion of this capability to all locations to ensure uniform protection to the United Nations network. Requested personnel are critical for the system’s initial configuration and operation
Inability to correlate data from multiple systems to determine trends in activity and reference historical (logged) system data. Lack of visibility	Continuous monitoring (log analysis)	The system collects logs of many systems to find trends of attacks across the network and provides quick access to locate the history of an attack when it is found. The system is critical to establish the overall use of all security systems. Requested personnel are critical for the system’s initial configuration and operation

Issue	*Solution*	*Description*
Lack of resources to properly determine the sources of attacks and the full extent of damage associated with an information breach	Malware, forensics and incident response	Requested personnel will provide the capacity to quickly examine what information may be lost after a breach, or the mechanism of attack, thus supplementing and increasing the skillset of United Nations staff in this area
Lack of compliance, updates and patching of United Nations systems globally leads to a higher level of vulnerability	Vulnerability assessments	Continued monitoring and checking of compliance through the use of automated software to ensure that all United Nations systems are “up to date” and to determine remaining vulnerabilities

Annex II

Estimated annual and total expenditures on information and communications technology (ICT) since 2010

(In United States dollars)

	Biennium 2010-2011			*Biennium 2012-2013*		
	2010	*2011*	*Total*	*2012*	*2013*	*Total*
Posts	318 000.00	318 000.00	636 000.00	719 600.00	773 450.00	1 493 050.00
Consultants		177 221.00	177 221.00	112 777.00		112 777.00
Training				436.67		436.67
ISO 27001 consultant travel				14 130.00	2 995.00	17 125.00
Independent security assessments					60 000.00	60 000.00
ISO 27001 assessments	24 000.00	33 025.49	57 025.49	38 170.90	1 545.00	39 715.90
Specialized server protection software		64 276.10	64 276.10	7 122.15	7 122.15	14 244.30
Endpoint protection software	4 144.50	193 435.18	197 579.68	234 711.39	300 611.97	535 323.36
Governance and compliance software				19 703.00		19 703.00
Advanced e-mail filtering solution for United Nations Headquarters					200 000.00	200 000.00
Firewalls for United Nations Headquarters				307 968.80	540 000.00	847 968.80
Additional ICT action plan measures					715 158.00	715 158.00
Total	**346 144.50**	**785 957.77**	**1 132 102.27**	**1 454 619.91**	**2 600 882.12**	**4 055 502.03**

Annex III

Expenditures incurred for information security during the biennium 2012-2013

(In United States dollars)

Item	*Name*	*Description*	*Price*	*Quantity*	*Total*
1.	**Short order purchase order items (<4,000)**				
	Manual web security testing software	Integrated platform for performing Security testing of web applications. Unique with many manual, professional oriented features to be used by advanced testers. Low cost, high value tool	300	2	600
	Basic vulnerability scanning software	Automated network/server vulnerability analysis tool — low cost, allows the use of multiple servers	3 900	1	3 900
	Intelligence and analytics tools	Open source intelligence and forensics application, with casefile application	760 + 200	1	960
	Forensics software	Leading forensics toolkit can be used on desktops, servers and mobile devices	2 999 + 599	1	3 598
	Hard drive forensic tool	Used to externally connect SATA hard drives to a PC for copy and/or forensic work	75	2	150
	Subtotal				**9 208**
2.	**Request for quotation items (<40,000)**				
	Website testing security scanner tool	Automated website security testing/analysis software tool	5 950	1	5 950
	Website testing security analysis tool	Automated website security testing/analysis software tool	20 300	1	15 000
	Firewall management software	Software for firewall rule management and tracking	35 000	1	35 000
	Subtotal				**55 950**
3.	**Invitation to bid items (<30,000-200,000)**				
1	Contractual services (firewall expert)	Securing of external consultant for support of network redesign and firewall implementation. 1 month time in late Nov., early Dec.	40 000	1	40 000
	Subtotal				**40 000**

Item	*Name*	*Description*	*Price*	*Quantity*	*Total*
4.	**Request for proposal items (Ongoing, varying)**				
	Information security awareness course	Development of an information security awareness module in HTML5 for use in Inspira	30 000	1	30 000
	Advanced e-mail filtering system	Provision of fire eye e-mail MPS appliances and software, including professional services for advanced e-mail filtering	230 000	1	230 000
	Checkpoint layer 7 firewalls	Purchase of multiple checkpoint layer 7 firewalls and add-on blades	540 000	1	540 000
	Managed security services	Procurement of multiple-year contract for managed security services, including hardware, software and outsourced security expertise for network monitoring	350 000	1	350 000
	Subtotal				**1 150 000**
	Grand total				**1 255 158**