United Nations A/61/566

General Assembly

Distr.: General
9 November 2006

Original: English

Sixty-first session
Agenda items 117, 129 and 130

Programme budget for the biennium 2006-2007

Financing of the International Criminal Tribunal for the Prosecution of Persons Responsible for Genocide and Other Serious Violations of International Humanitarian Law Committed in the Territory of Rwanda and Rwandan Citizens Responsible for Genocide and Other Such Violations Committed in the Territory of Neighbouring States between 1 January and 31 December 1994

Financing of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991

Strengthened and unified security management system for the United Nations: standardized access control

Report of the Secretary-General

Summary

At its sixtieth session, the General Assembly decided to defer to its sixty-first session consideration of standardized access control, as proposed by the Secretary-General in his report of 24 February 2006 (A/60/695) considered by the Advisory Committee on Administrative and Budgetary Questions in its report of 7 March 2006 (A/60/7/Add.35). The present report is submitted to further elaborate on standardized access control measures as outlined in the report of the Secretary-General and to provide the detailed information requested by the Advisory Committee in its report. It also describes the proposed scope, concept and revised course of action for standardized access control at all main locations of the Organization, as requested by the General Assembly in its resolution 59/294. Furthermore, as requested by the Assembly in paragraph 44 of section XI of its resolution 59/276, it recalls the estimated costs as proposed in the report of the Secretary-General for addressing critical requirements that should be implemented

06-61012 (E) 141106

without delay. The additional improvements identified will bring all main duty stations into compliance with the headquarters minimum operating security standards for perimeter protection and electronic access control. The report sets a new timetable for a detailed plan for implementation of the project.

I. Introduction

1. Pursuant to paragraph 44 of section XI of General Assembly resolution 59/276, the Secretary-General submitted his report of 24 February 2006 (A/60/695), in which he outlined the proposed scope, concept and revised course of action for standardized access control at all main locations of the Organization. The Secretary-General has proposed that the implementation of the standardized access control project be undertaken in two phases. The first phase of standardized access control is intended to meet compliance with headquarters minimum operating security standards for perimeter protection and electronic access control. The second phase is designed to provide for compliance with those standards with regard to defined layers of security within the perimeter. In his report, the Secretary-General stated that a second report would be submitted to the Assembly at its sixty-first session, containing a detailed plan and estimated resource requirements. In its decision 60/551 B, the General Assembly decided to defer to its sixty-first session consideration of the standardized access control project proposed in the report of the Secretary-General. In line with that decision and as requested by the Advisory Committee on Administrative and Budgetary Questions in its report of 7 March 2006 (A/60/7/Add.35), the present report of the Secretary-General provides additional information on the first phase of the project. The second phase will be presented to the Assembly at its sixty-second session.

2. During 2005, the Department of Safety and Security of the Secretariat, through a team of experts, undertook a comprehensive assessment of the security position at each of the eight main locations of the Secretariat and at the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991 and the International Criminal Tribunal for the Prosecution of Persons Responsible for Genocide and Other Serious Violations of International Humanitarian Law Committed in the Territory of Rwanda and Rwandan Citizens Responsible for Genocide and Other Such Violations Committed in the Territory of Neighbouring States between 1 January and 31 December 1994. The expert team consulted information technology and facility management experts as well as security personnel at each location in the course of the comprehensive assessment. Those visits were the first opportunity for the Department to augment earlier reports with a comprehensive on-site survey of all the locations.

3. The experts noted that substantial security improvements had been made in the context of a large number of ongoing projects aimed at strengthening security and safety over the past two years. No redundant or overly elaborate projects in excess of requirements, as determined by local conditions, were identified by the experts. However, the team noted some delays in project implementation, as well as shortfalls at certain locations in connection with security coverage or in the technical parameters of particular barriers, perimeter surveillance or other access control measures. The team attributed those shortcomings in part to insufficient security capacity owing to a lack of project management caused by a delay in recruitment against authorized security posts at the Professional level. The expert team also identified specific instances at some locations where technical measures, either in place or planned, required upgrading or adjustment.

4. In its findings, the team of experts proposed that the various sets of minimum operating security standards currently in use, including the headquarters minimum

operating security standards, be consolidated by the Department of Safety and Security into a single set of operational instructions that would incorporate additional details, while adding flexibility by setting out mandatory as well as recommended requirements. This is now under way. Through the project access control team, the Department would provide local managers with technical advice on a case-by-case basis and propose appropriate security standards to them, thereby avoiding unnecessary delays in the implementation of projects already under way. A time frame of six to eight months was proposed by the team for procurement and preliminary design. The project bid and construction phase was estimated to require 18 to 24 months. Full project duration from procurement to commissioning and acceptance was estimated at 24 to 30 months from the time of approval by the General Assembly.

5. On the basis of the findings of the expert team, the Secretary-General proposed to defer implementation of the global identity management component as described in paragraph 26 of his report of 30 September 2004 (A/59/365/Add.1 and Corr.1), pending more detailed analysis of requirements and a feasibility study as to the cost benefits and operational value of that approach. The assessment would be made once the essential features of a standard access control system were in place.

II. Overview of existing access control capability

6. In his report of 5 April 2004 on strengthening the security and safety of United Nations operations, staff and premises (A/58/756), the Secretary-General outlined plans for security improvements to facility infrastructure, which included such projects as reinforcement of fences, traffic control barriers, security control centres, vehicle identification, remote closing and locking devices and the installation of blast-proof lamination on glass surfaces. Each of these projects has significantly improved the safety and security of the United Nations premises and each of the projects is consistent with the headquarters minimum operating security standards requirements and risk assessments. The projects reported on in annex II of the report of the Advisory Committee of 28 October 2004 (A/59/539) are still in various stages of implementation, with completion dates established for the present biennium.

7. The first phase of the proposed standardized access control project will provide for additional requirements for headquarters minimum operating security standards access control compliance with regard to the physical security of the perimeter. The second phase of the project, once approved by the General Assembly, will achieve full compliance with the headquarters minimum standards as regards access control by integrating the layers of security internal to the perimeter into the overall access control system. The first phase contains access control-related projects for the purpose of enhancing security capability. The standardized access control proposal for New York-based annex buildings and offices away from Headquarters is intended to resolve systematically the remaining weaknesses, which include deficiencies in coverage of access control, card readers and monitoring points; deficiencies in integration among systems such as closed-circuit television (CCTV), intrusion detection and access control; limited use of smart card technology; and no identity management.

8. An independent assessment was conducted of the technical soundness and cost-effectiveness of the proposed access control system. The assessment reviewed

the proposals with regard to the objectives of the headquarters minimum operating security standards and concluded that the proposed security improvements were fully compliant with those standards; the level of technology specified was appropriate and there was no overspecification of requirements; the overall design approach and the selection of technologies, systems and brands were consistent with standard practice in the security industry; and the cost estimates and unit costs of the access control system were accurate for budgetary purposes.

III. Expected results of access control

9. While significant progress has been made in reaching the headquarters minimum operating security standards, challenges remain because of various physical features of the perimeters. The standardized access control initiative is designed to achieve compliance with the headquarters minimum standards with regard to perimeter protection and electronic access control. The project aims to address those specific deficiencies, leading to a precise and definite result. The proposal includes additional enhancements to security for compliance with the standards of physical security measures that focus on perimeter security; use of electronic access cards (smart card technology); use of CCTV systems; use of alarms and intrusion detection; and integrated central monitoring of access control systems.

10. In the interest of cost-efficiency and security effectiveness, the implementation of the access control system focuses on the entry points into and perimeter of premises. However, the flexibility of that core system allows for system expansion as the need arises where additional layers of protection may be identified as being necessary and the appropriate security hardware installed cost-effectively. Future security enhancements can therefore be implemented incrementally.

11. The scope of the proposal focuses on those devices, hardware, software and databases that constitute a single system. Each device (camera, card reader, intrusion detection or vehicle barrier) is connected, controlled and monitored via the network. The operational advantages of such an approach are significant, because security personnel will be able to monitor and take action at the system level, having a complete picture of security throughout the premises.

12. The level of implementation will vary for each duty station. The costs of complying with the headquarters minimum operating security standards and implementing a standardized access control and identity system were determined after a detailed process of security assessment and gap analysis for the premises of each duty station. The current proposal of $23,683,000 reflects the resources needed to raise each duty station from its current security level to a level of compliance with the headquarters standards as regards access control, without redundancy or waste of expenditure.

IV. Details and implications of the standardized access control project

A. Management

13. As explained in paragraph 11 of the report of the Secretary-General of 24 February 2006 (A/60/695) with regard to the implementation of physical security measures, the Department of Safety and Security, the Department of Management

and administrative services at each main location share the respective responsibilities. Once projects have been completed and are operational, the offices away from headquarters, through the Department of Safety and Security, will manage the standardized access control system.

14. In paragraph 12 of the report, it was stated that an enhanced management structure, consisting of a senior-level steering group and the project access control team (see A/59/776) composed of security specialists and professionals with expertise in information technology and facility management would address the requirements of the site-specific plans at each main location.

15. In order to ensure that the project is fully tailored to specific conditions on the ground, including arrangements with host Governments, threat assessments and joint security arrangements at each location will be regularly updated in coordination with local law enforcement and security authorities. With the support of the project access control team, access control plans for each location are being verified in line with the standards of the Department of Security and Safety and care is being taken to ensure that those responsible for on-site procurement and implementation will receive the necessary technical security advice, guidance and assistance.

B. Integration with projects approved by the General Assembly in previous resolutions

16. The present report is submitted in the context of the many resolutions adopted by the General Assembly from the fifty-sixth session onwards, focusing on the strengthening of the safety and security of United Nations operations, staff and premises. The proposed project is consistent with the strategy and objectives of those resolutions and is designed for full integration with fully implemented and pending projects. The standardized access control system presented in the report of the Secretary-General of 5 April 2004 (A/58/756) and approved by the General Assembly in its resolution 58/295 is an integral component of the collective strengthened and unified security management system for the United Nations and will be fully integrated with the standardized access control project.

C. Integration with approved safety and security projects

17. Several resolutions and reports are relevant to the integration of access control: resolution 56/286, in which the General Assembly approved the Secretary-General's proposed long-term measures for strengthening the security and safety of United Nations premises; long-term measures related to the areas of security and safety of the premises/building and property management (A/56/848); resolution 58/295, on the revised estimates for the infrastructure projects of Phase I; and the significant enhancements to the minimum operating security standards as specified in the Secretary-General's report (A/58/756).

18. At the request of the Advisory Committee on Administrative and Budgetary Questions (see A/60/7/Add.35), a synopsis of previously funded projects that would integrate seamlessly with the standardized access control system is provided in the following table:

Duty station	*Funded project*
United Nations Office at Geneva	• Creation of a security control centre with provision for adequate technical and communications support
	• Provision of full perimeter protection, including reinforcement of fences, traffic control barriers and access control at the Palais des Nations Gate and the Chemin de Fer Gate, modification of road access to the gates and installation of a new generalized video surveillance system
	• Improvement of the intermediate area surveillance, including lighting and video surveillance in the underground garage area
	• Installation of air and water intake protection structures
	• Upgrading of the public address system for emergency announcements
United Nations Office at Vienna	• Increase in threat-prevention measures, in particular along the site perimeter and service areas
	• Installation of perimeter fence surveillance and an alarm system
	• Constructional reinforcement of perimeter gates and posts, including vehicle crash barriers
	• Installation of remote closing and locking devices for building access
	• Installation of a vehicle recognition system and screening equipment for vehicle search
	• Installation of a stationary monitoring system for radioactive material
	• Installation of a heating, ventilation and air-conditioning system access control, protection and alarm system
	• Upgrading of the Security Control Centre
United Nations Office at Nairobi	• Establishment of a pre-registration area at the visitors' pavilion to screen delegates before allowing them into the complex
	• Additional improvement of gates and barriers and reinforcement of the perimeter fence
	• Construction of a registration booth for conference participants in the visitors' pavilion
	• Earth work and civil work for barriers, turnstiles and planter boxes around the entrance to the complex
	• Relocation and construction of new security booths
Economic Commission for Africa	• Enlargement of the visitors' entrance area, including the provision of a covered pavilion and access gates for the handicapped, and installation of a revolving turnstile
	• Construction of a small building for registration of conference participants outside the main entrance to improve access control

Duty station	*Funded project*
	• Construction of premises for an off-site pass, identification and accreditation centre
	• Improvements to physical security and reinforcement of the existing perimeter wall
	• Construction of a new perimeter security wall around the additional land granted by the host Government
	• Upgrading of the closed-circuit television system (CCTV) at the United Nations Conference Centre and installation of a CCTV perimeter intrusion detection system
	• Installation of a fire alarm notification system in the office buildings
Economic and Social Commission for Asia and the Pacific	• Upgrading of surveillance and preventive measures, including expansion of the existing video surveillance system to encompass the entire perimeter of the complex; modification of the fire sub-control centre to integrate all CCTV cameras and all motion detectors into the building automation system; and installation of infrared motion detectors around the entire perimeter of the complex and improvement of lighting in the garage
	• Installation of four hydraulic vehicle barriers at all major entrances and installation of 20 static bollards to prevent vehicle ramming at vulnerable perimeter locations
	• Installation of an automatic vehicle bomb scanning system at the main entrance
	• Installation of an intruder alarm system for all fire escape doors and access ways to the buildings
	• Upgrading of the CCTV system, including computerizing the control centre for improved monitoring and coverage
Economic Commission for Latin America and the Caribbean	• Upgrading of the lighting, alarm and video surveillance systems
	• Construction of an off-site pass and identification centre at the southern entrance area of the Commission complex
Economic and Social Commission for Western Asia	• Upgrading of protective measures, including installation of a fence and sliding doors to provide protection from demonstrators and threats from the street, as well as intrusion from adjacent buildings; installation of video surveillance equipment in the garage and service lift and on the roof of the building to protect against intruders; and installation of lighting on the perimeter wall
	• Construction of a screening area

19. These previously funded initiatives as proposed by the Secretary-General (see A/58/756) represented urgent initial measures, but they have left gaps in compliance

with the headquarters minimum operating security standards. The goal of the present proposed standardized access control project is to fill those gaps. The end result is a compliant integrated perimeter protection and electronic access control system.

D. Integration with the overall United Nations information technology strategy

20. In paragraph 44 (a) of section XI of its resolution 59/276, the General Assembly mandated the integration of the standardized access control system with other projects approved by it in previous resolutions, including those being implemented in the context of the overall information technology strategy. Information technology security, disaster recovery, business continuity and crisis management are broader issues that, while outside the scope of the standardized access control project, may have an impact on the project by imposing new requirements for data links or technological applications. The Department of Safety and Security will therefore continue to maintain close coordination with the Information Technology Services Division of the Department of Management in order to ensure compliance of ongoing, intended or future access control and other security activities or systems with the overall United Nations information technology strategy. Integration with that evolving strategy in connection with reform initiatives will also be taken into consideration throughout the life cycle of the project. The project access control team project management structure, consisting of multiple service areas to include information technology offices, will ensure that the necessary service-level interfaces are incorporated into all access control systems.

E. Impact on human resource requirements

21. In paragraph 44 (b) of section XI of its resolution 59/276, the General Assembly requested an assessment of the impact of implementing the standardized access control system on human resource requirements in the area of safety and security. The impact of implementing the system on human resource requirements, specifically security officers, is negligible. Although the system is an information technology-based system, it is not an automation system replacing functions or reducing manpower requirements, but rather an essential capability-enhancing tool to security personnel serving as the “eyes and ears” of the perimeter.

22. With reference to the report of the Advisory Committee on Administrative and Budgetary Questions of 28 October 2004 (A/59/539), the standardized access control project strategy is consistent with the Organization’s commitment to make full use of technological achievements that could reduce dependence on human resources. The implementation of a robust access control capability is an example of that commitment. With the appropriate deployment of technology, security personnel are no longer subject to the challenge of being at the right place at the right time in the event of an incident. Instead, a well-integrated surveillance and intrusion detection system gives security officers an effective detection and response capability.

23. The implementation of a standardized access control system does require a small cadre of specialized and dedicated staff. The human resource requirement is

necessary to meet the requirements of sustained operations and maintenance round the clock. The access control system is a mission-critical system serving as a backbone to the physical protection capability of the premises. It requires a fail-safe operation round the clock. To that end, the need for specialized technical support is anticipated, which will be fully analysed and included in the scope of review for the second phase of the standardized access control project.

F. Individual characteristics of each United Nations headquarters and main duty station

24. In formulating proposals for the access control system, global standards have been adopted for technologies, equipment and design to leverage economies of scale, bring down maintenance costs, improve maintenance and build a common pool of skills. However, the estimates also reflect the diversity among the environments of the duty stations and their differing requirements. The proposals are thus not generic, but tailored to the specific requirements of each duty station to ensure compliance with the common minimum standards prescribed by the headquarters minimum operating security standards, using a standard technological framework.

25. The basis for the proposal is that the unique requirements for each duty station campus, taking into account existing investment, the campus environment, gap analysis and localized costs such as labour, were assessed for each campus and costed accordingly. Current compliance with the headquarters minimum operating security standards for perimeter protection and electronic access control varies for each duty station based on two factors: (a) the unique nature of the campus; and (b) previous investment in physical security. The proposal accounts for these two factors in addressing the requirements of each campus with respect to existing implementation. The most noteworthy difference among campuses will be the equipment and installation requirements for the physical layout of the campus. A survey of the individual characteristics of each United Nations headquarters and main duty stations is presented in paragraphs 26-55.

G. Economic Commission for Africa

26. The Economic Commission for Africa (ECA) complex in Addis Ababa consists of seven buildings spread over an area of 27.3 acres. Apart from the offices of the Economic Commission for Africa, the complex accommodates the offices of 14 other United Nations entities.

27. The duty station does not use electronic identity (ID) cards and is therefore not equipped with card reader devices, access control software or electronically controlled hydraulic barriers. The campus currently has 122 CCTV cameras installed, but they are backed up to video home system (VHS) tape recorders and proprietary video recorders. CCTV is not integrated with an access control system. Additional cameras are proposed to cover areas of the perimeter and sensitive locations that are not provided for under the existing installation. Previously installed cameras will be fully integrated with the proposed access control system.

28. The proposal is based on the installation of card reader devices on perimeter doors, hydraulic vehicle barriers, badging stations, cameras, lighting to support the

perimeter, access control software and a redesigned security control room with system integration and monitoring.

H. Economic Commission for Latin America and the Caribbean

29. The main premises of the Economic Commission for Latin America and the Caribbean (ECLAC) in Santiago currently have very limited access control systems in place. The duty station does not use electronic ID cards or hydraulic vehicle barriers and its perimeter of 14.18 acres is not equipped with intrusion detection and alarm systems. The CCTV system consists of 32 cameras, which do not adequately cover the perimeter and are not integrated with a security control centre. CCTV video is backed up via tapes. The perimeter lighting was upgraded during the biennium 2002-2003 but remains insufficient. The power back-up capacity, however, is adequate.

30. The proposal is based on the installation of card reader devices on perimeter doors, hydraulic vehicle barriers, badge-making stations, additional cameras, lighting to support the perimeter, access control software and a redesigned security control centre with system integration and monitoring for the main ECLAC premises in Santiago. Regional centres will be considered in the second phase of the standardized access control project.

I. Economic and Social Commission for Asia and the Pacific

31. The Economic and Social Commission for Asia and the Pacific (ESCAP) complex consists of three buildings, including a conference centre, occupying an area of 7.8 acres near to several government offices. The duty station does not use electronic ID cards and is therefore not equipped with card reader devices, access control software or electronically controlled hydraulic barriers. The location currently has CCTV installed; however, it is recorded on VHS tape recorders and proprietary video recorders. CCTV is not integrated with any access control system. Additional cameras are proposed to cover areas of the perimeter and sensitive locations that are not provided for under the existing installation. Previously installed cameras will be fully integrated with the proposed access control system.

32. The proposal is based on the installation of card reader devices on perimeter doors, card badging stations, cameras, access control software and a redesigned security control centre with system integration and monitoring.

J. Economic and Social Commission for Western Asia

33. The United Nations House/Economic and Social Commission for Western Asia (ESCWA) Building is located in the Central District of Beirut and is one of the main buildings in Riad el-Solh Square. The total area of the compound amounts to 10.7 acres. The duty station uses electronic ID cards and is therefore equipped with some card reader devices, access control software and two electronically controlled hydraulic vehicle barriers. The access control software is an old version in need of an upgrade. The location currently has 73 CCTV cameras installed; however, they are backed up to a single proprietary video recorder that is not integrated with the access control system. Additional cameras are proposed to cover areas of the perimeter and sensitive locations that are not provided for under the existing

installation. Previously installed cameras will be fully integrated with the proposed access control system.

34. The proposal is based on the installation of hydraulic vehicle barriers, card reader devices, card badging stations, cameras, access control software and limited redesign of a security control centre with integration and monitoring.

K. New York: annex buildings

35. The United Nations Headquarters premises in New York consist of the United Nations Secretariat and 12 annex buildings, all in close proximity. The annex buildings account for an area of approximately 20 acres. In many cases, security for the annex buildings is provided by the Division of Headquarters Security and Safety Services of the Secretariat during business hours and by the landlord after business hours.

36. The scope of the proposal is to secure the points of ingress into and egress from the annex buildings by the migration of the existing security systems to the United Nations global standard for access control and video. A broad approach was taken to include the specific electronic security needs of the various occupants and the workplace environment in each of the locations. The first phase of project implementation will cover the three annex buildings mentioned below as they have the greatest gap between existing conditions and the headquarters minimum operating security standards.

37. Recommendations for security monitoring and controls take into account that the United Nations is, in most cases, one of many tenants in a building that is owned and operated by an unrelated landlord.

1. Falchi Building

38. The Falchi Building in Long Island City, New York, is geographically removed from Headquarters and has no identification on the facade of the building to indicate to the general public that it houses United Nations premises. Security for the building is provided by the landlord. The United Nations occupies two floors of the warehouse building and the space is used as file storage for the Secretariat. The scope of the proposal is to secure ingress and egress points and to migrate the existing system to United Nations global standards for access control and video.

39. The proposal is based on the provision of security devices as follows: cameras, door contacts, request-to-exit motion detectors, card readers, electromagnetic locks and integration with the Headquarters access control system.

2. FF Building on East 45th Street

40. The FF Building is very close to the Headquarters premises, but is not identified on the outside as United Nations premises. Security for the building is provided in the lobby by United Nations security personnel during normal business hours and by the landlord after hours. There is coverage around the clock.

41. The FF Building is split between three occupants: the United Nations Secretariat and the United Nations Development Programme, which between them occupy 95 per cent of the building, and a third-party magazine not affiliated with the United Nations.

42. The proposal is based on the provision of security devices for both the tenant and landlord space as follows: turnstiles, magnometers, cameras, door contacts, door releases, request-to-exit motion detectors, card readers, electromagnetic locks and integration with the Headquarters access control system.

3. UNITAR Building

43. The UNITAR Building is very close to the Headquarters premises and is identified on the outside for the general public as "The United Nations Institute for Training and Research". Security for the building is provided in the lobby by United Nations security personnel during normal business hours only.

44. The Secretariat occupies the entire UNITAR Building. The second to fifth floors are general office spaces, while the first floor is the United Nations badge-making area, which houses documentation and passes for access onto Headquarters premises and is protected only by glass windows and camera.

45. The proposal is based on the provision for security devices as follows: cameras, door contacts, door releases, request-to-exit motion detectors, card readers and integration with the Headquarters access control system.

L. United Nations Office at Geneva

46. The costs estimated for the United Nations Office at Geneva (UNOG) pertain to the Palais des Nations and the Palais Wilson. The security requirements for standardized access control for the new G. Motta Building for the Office of the United Nations High Commissioner for Human Rights were described in the Secretary-General's report (A/60/899) and were approved by the General Assembly in its decision 60/562. The costs estimated do not include the annex buildings serviced by the UNOG Security and Safety Section and occupied by organizations funded from extrabudgetary resources. The plan layout of the two sites is as follows: the Palais des Nations has a total area of 111.20 acres, a perimeter of 10,498 feet, with 16 occupied buildings and 3 storage buildings; the Palais Wilson has a building area of 2.42 acres. The duty station does not use electronic ID cards for entry to the premises and is therefore not equipped with card reader devices or access control software in these locations. There are six electronically controlled hydraulic vehicle barriers in place for some of the entrances.

47. The uniqueness of the UNOG premises has a significant impact on the resources required for the access control project. The land is not flat and the perimeter is encircled with large trees and thick foliage. Added to this is the large distance between the perimeter and the buildings. Currently there are 92 camera positions located at the gates and at limited areas in the Palais des Nations. The existing cameras are not integrated with any access control system.

48. The high number of cameras required includes full perimeter coverage as well as coverage of the intermediate areas (which are wooded and therefore require more cameras to achieve line of sight for a given area). All 49 entry points into the building, as well as six other buildings within the UNOG premises, will also have camera surveillance. Added to this are the multiple locations of high security areas that need to be monitored (e.g. executive offices of the organizations inside the Palais des Nations, power stations, server rooms, archives, museum and so on). The entry points, secure areas and conference areas will also require differing levels of access control, hence the need for a substantial number of card readers and

turnstiles. The gross requirement has been significantly reduced after taking into account the approved projects related to perimeter protection and surveillance of intermediate areas.

49. The proposal is based on the installation of card reader devices, card badging stations, cameras and access control software and a redesigned security control centre with system integration, and monitoring with digital backbone to provide connectivity for the system.

M. United Nations Office at Nairobi

50. The United Nations Office at Nairobi (UNON) complex consists of an area of 163 acres; the length of the perimeter is 13,451 feet. There are 37 buildings, comprising a total office and conference centre space of 10 acres. The duty station does not use electronic ID cards and is therefore not equipped with card reader devices, access control software or electronically controlled hydraulic barriers.

51. The proposal is based on the installation of cameras, lighting, card reader devices, turnstiles, hydraulic vehicle barriers, card badging stations, access control software and a redesigned security control centre with system integration and monitoring.

N. United Nations Office at Vienna

52. The Vienna International Centre is the property of the Government of Austria and is leased by the United Nations. It occupies a total land area of 44 acres. The duty station uses electronic ID cards for entry to the premises but is not equipped with adequate card reader devices or access control software; the system is to be fully implemented under the first phase. There are 13 barriers installed, but they are not integrated with an access control system. The premises currently have a CCTV installation, but it does not cover the perimeter area and is not integrated with an access control system. The addition of 24 cameras is proposed to cover areas of the perimeter. Previously installed cameras will be fully integrated with the proposed access control system.

53. The proposal is based on the installation of cameras, card reader devices, card badging stations, access control software and a redesigned security control centre with system integration and monitoring.

O. Implications for the capital master plan

54. In paragraph 44 (d) of section XI of its resolution 59/276, the General Assembly requested the Secretary-General to report on the implications of the global access control system for the capital master plan. It should be recalled that, by its resolution 56/286, the Assembly moved forward from the capital master plan the implementation of a complex-wide access control project at Headquarters, as proposed by the Secretary-General (see A/56/848, annex I, para. 40 (b) (ii), and annex II). The related measures included the reinforcement of perimeter protection and the installation of surveillance, monitoring and preventive measures linked to a security command centre. That project has been largely implemented. Given that the physical security requirements of the main Secretariat complex are fully addressed through the capital master plan project, the proposed standardized access control

project in the case of Headquarters applies to only three Headquarters annex buildings. In that connection it should be noted that the capital master plan-managed project at the main Secretariat complex has been designed for full compatibility with the standardized access control project discussed in the present report.

P. Management of identity information

55. Although the global identity management component will be deferred for further analysis, the need for proper management of local identity repositories is vital. Local identity management systems will be governed by a strict policy and procedural framework aimed at ensuring due diligence and appropriate protection of sensitive data. A management and policy framework is clearly established for the principles and guidelines for sharing the information obtained through the system. The report of the Secretary-General on an information and communications technology strategy (A/57/620) and the Secretary-General's bulletin on the use of information and communications technology resources and data (ST/SGB/2004/15) make specific provisions for the security of the system and the safeguarding of sensitive information. The strategy applies basic staff rules for the sharing of access control and identity-related information ensuring that the access to or possession or distribution of sensitive data is in accordance with all regulations, rules and administrative issuances applicable to such sensitive data.

56. The policy further establishes the norms for safeguarding and accountability of staff for preserving the confidentiality of sensitive information and forbids making sensitive information and communications technology data available to persons who have not been authorized to access the data.

57. Access to identity information, in particular records relating to entering into and exiting from the facility, are deemed "confidential" and "vital", and are therefore limited in dissemination. Access will be on a formally certified need-to-know basis or on the basis of an emergency requirement. For the purpose of emergency preparedness and recovery operations, the system will record entry and exit of persons. This requirement is now common practice as a result of the events of 11 September 2001 at the World Trade Centre. It is critical, in emergencies, for the Organization to be able to establish the presence or absence of persons on the premises. The information is recorded for this sole purpose.

58. The concern for privacy has not been neglected, is preserved and will be enforced by policy. It is important to note that the types of information shared through the system, as mentioned, will be strictly identity data (e.g. name, duty station, access level and so on) and not records relating to the movement of the named person. Access control records relating to entry, exit and movement within the premises are not shared except in the event of an emergency.

59. In the interest of transparency and accountability, the Secretariat is committed to make the architecture, database and associated procedures protected and secured from sharing of identity data. This includes the enforcement of specialized policies for data relating to delegates. As stated in the Secretary-General's bulletin of 29 November 2004 (ST/SGB/2004/15), the Office of Internal Oversight Services is empowered to review and when necessary conduct investigations into the use, sharing and accessing of identity data and processes.

V. Financing and time frame for implementation of the project

60. As mentioned above, it is foreseen that the implementation of the standardized access control project will be undertaken in two phases. During the first phase it is intended to rectify all the shortcomings and gaps in physical security identified during the project reassessment process undertaken in 2005. Those requirements are described in summary form in the table below, by duty station and function or project. All items listed are to be implemented during the first phase, noting that, in line with ongoing security changes in duty stations, a redistribution of individual amounts within duty stations may be necessary. The related costs are estimated at $23,683,000, as proposed in the previous report of the Secretary-General (A/60/695), for which authorization is sought in order for the Secretary-General to enter into commitments to be reported in the context of the relevant second performance reports for the tribunals and the programme budget for the biennium 2006-2007.

Estimated resource requirements for the first phase of the project, by duty station and function or project

(Thousands of United States dollars)

Duty station	*Perimeter intrusion*	*Closed-circuit television*	*Access control barriers*	*Identification server and badging stations*	*Security control room*	*Total*
Geneva	150.0	150.0	—	675.0	946.6	1 921.6
Vienna	210.0	100.0	176.6	525.0	1 100.0	2 111.6[a]
Nairobi	—	1 862.9	2 200.0	425.0	600.0	5 087.9
Addis Ababa	439.4	650.0	950.0	425.0	1 150.0	3 614.4[b]
Santiago	750.0	800.0	577.5	425.0	600.0	3 152.5
Bangkok	—	245.0	—	375.0	325.0	945.0
Beirut	100.0	325.0	1 250.0	375.0	125.0	2 175.0
New York annex buildings	—	—	—	—	—	1 200.0[c]
Subtotal	**1 649.4**	**4 132.9**	**5 154.1**	**3 225.0**	**4 846.6**	**20 208.0**
International Tribunal for the Former Yugoslavia	100.0	—	950.0	325.0	125.0	1 500.0
International Criminal Tribunal for Rwanda	550.0	—	950.0	400.0	75.0	1 975.0
Subtotal	**650.0**	**—**	**1 900.0**	**725.0**	**200.0**	**3 475.0**
Total	**2 299.4**	**4 132.9**	**7 054.1**	**3 950.0**	**5 046.6**	**23 683.0**

[a] $2,111,600 is the gross provision for Vienna. Under the regular budget, the portion of cost attributable to the United Nations under the cost-sharing arrangements is $458,428.

[b] In addition, estimated requirements in the amount of $417,300 for the access control system to be installed in the new office building at the Economic Commission for Africa (see A/60/532, para. 19) would be needed at a later stage.

[c] Urgent security measures for the UNITAR, FF and Falchi Buildings.

61. Subject to approval by the General Assembly of the proposed concept, scope and revised course of action for the project as reflected in the present report, during the first phase of project implementation it is also foreseen that the project will be fully developed on a site-by-site basis and that a detailed project implementation plan for the second phase will be submitted to the Assembly at its sixty-second session. Projects during the second phase would complete the security access control strategy by closing all headquarters minimum operating security standards access control gaps. Components of the second phase are directed at the inner circles of protection, which include but are not limited to building doors, windows and roofs, conference and meeting rooms, critical infrastructure rooms, elevator cars and lobby controls, highly secure offices, archival and special storage areas and parking garages. Access control devices would include but not be limited to CCTV, optical portals, revolving doors, door alarms, intrusion detection, emergency intercoms and panic alarms. All devices would be fully integrated into the existing central monitoring control centres. The second phase would also include closing the headquarters minimum operating security standards gap for all annex buildings at Headquarters, to be carried out on a cost-shared basis with the United Nations funds and programmes that are tenants of the buildings, the full project cost estimates and financing arrangements. Similarly for the United Nations Office at Vienna, the two phases of standard access control will be carried out on a cost-shared basis with the other United Nations entities housed in the complex.

62. The second phase of project implementation would begin only after consideration of and approval by the General Assembly of the project proposals to be submitted to it at its sixty-second session. Detailed cost estimates for the second phase cannot be made until the elements of the first phase have begun. It is estimated that the completion time of the entire project will be between 24 and 30 months, to include a design phase of 6 to 8 months and an implementation phase of 18 to 24 months from the date of approval by the Assembly of the implementation plan and relevant financing arrangements.

VI. Conclusions

63. **Following the review and assessment of the current status of access control at all main locations of the Organization, a two-part approach for implementation of the standardized access control system is proposed. In the first phase, measures will be taken to rectify identified shortcomings and gaps in perimeter protection and electronic access control at all main locations. The total related estimated requirement of $23,683,000 is proposed to be met by commitment authority to be reported in the context of the second performance reports for the tribunals and the programme budget for the biennium 2006-2007.**

64. **The second phase of the standardized access control project will achieve full access control compliance with the headquarters minimum operating security standards. Specifically, the second phase of standardized access control is designed to provide a full package of access control measures of protection beyond the perimeter layer and into the multiple internal layers of protection. This would include but not be limited to building doors, windows and roofs, conference and meeting rooms, critical infrastructure rooms, elevator cars and lobby controls, highly secure offices, archival and special storage areas and**

parking garages. Access control devices would include but not be limited to CCTV, optical portals, revolving doors, door alarms, intrusion detection, emergency intercoms and panic alarms. All devices would be fully integrated into the existing central monitoring control centres.

65. **Included in the plan will be capacity for technical security advice and support, a defining of the scope and approach for standardization, a procurement strategy based on standardization of systems and equipment while allowing for serviceable local variations, advice and support for system maintenance and identification of the impact of the standardized access control system on human resource requirements in the area of safety and security.**

VII. Action required by the General Assembly

66. **The General Assembly is requested:**

(a) To approve the proposed course of action;

(b) To authorize the Secretary-General to enter into commitments of $20,208,000 under the programme budget for the biennium 2006-2007, $1,500,000 under the budget for the International Tribunal for the Former Yugoslavia and $1,975,000 under the budget for the International Criminal Tribunal for Rwanda, to be reported on in the context of the respective second performance reports.