

Distr.: General 11 October 2022

Original: English

Seventy-seventh session Item 138 Proposed programme budget for 2023

## **Capital investment planning**

### **Report of the Secretary-General**

### Summary

The present report on capital investment planning is submitted pursuant to General Assembly resolution 76/245, in which the Assembly endorsed several recommendations of the Advisory Committee on Administrative and Budgetary Questions in its first report on the proposed programme budget for 2022 (A/76/7).

The General Assembly has requested comprehensive and detailed information on information and communications technology (ICT) spending globally across the Secretariat, including ICT capital expenditures and a capital investment plan, investments to support new modalities of work, upgrades and enhancements to the standardized access control systems for physical security, a comprehensive action plan for dealing with cybersecurity, ongoing and planned projects to improve the accessibility of premises, and investments in conference facilities to deal with the impact of the coronavirus disease (COVID-19) pandemic.

The present report contains information in section II on global ICT spending across all funding sources, and a preliminary analysis of ICT assets and equipment, in order to establish baselines before considering investment proposals. Section III includes proposals to expand both the scope and scale of coverage of the Secretariat's cybersecurity programme of work to ensure that it is suitable for managing the cyberthreats confronting the Organization.

Section IV contains the results of an assessment of physical security arrangements at Headquarters, offices away from Headquarters and the regional commissions and provides, for informational purposes only, a preliminary estimate of investments needed over 11 years, without necessarily identifying any funding gaps at this stage. Section V contains a description of the work undertaken to assess the need for upgrades to buildings and facilities at these locations, including in relation to local ICT infrastructure, the accessibility of premises and upgrades to conferencing facilities, among other things.





The General Assembly is requested to: (a) take note of the report of the Secretary-General; (b) approve the establishment of four posts (P-4) and six general temporary assistance positions (3 P-2 and 3 General Service (Principal level)); and (c) appropriate, under the proposed programme budget for 2023, an amount of \$6,662,700 for cybersecurity and an amount of \$5,488,000 for urgent upgrades to the safety and security infrastructure at the Economic Commission for Africa to ensure compliance with minimum operating security standards.

### I. Introduction

1. In its resolution 76/245, the General Assembly endorsed several recommendations of the Advisory Committee on Administrative and Budgetary Questions requesting comprehensive information on information and communications technology (ICT) spending globally across the Secretariat, including ICT capital expenditures and investments to deal with new modalities of work, a capital investment plan for ICT and a comprehensive action plan relating to cybersecurity. The Assembly also endorsed the Advisory Committee's recommendations requesting consolidated information on upgrades and enhancements relating to standardized access control for physical security, investments relating to conference facilities and ongoing and planned projects to improve the accessibility of premises.

2. The present report outlines the actions being taken in relation to ICT, physical security, cybersecurity and the upgrades of buildings and facilities, including for conference management, accessibility, sustainability and business continuity. While ICT and cybersecurity have been considered globally for the Secretariat, at this phase physical security requirements have been assessed only for United Nations Headquarters, offices away from Headquarters and the regional commissions. Requirements for buildings and facilities are also similarly limited in this phase to these locations. However, for each location, the requirements are being considered holistically, and factor in potential standardization that may be forthcoming or needed across the entire Organization.

### **II.** Information and communications technology

3. In paragraph 11 of its resolution 75/252, the General Assembly stressed the importance of aligning ICT investment with the Secretary-General's vision of a digital United Nations and addressing the need for business continuity during the coronavirus disease (COVID-19) pandemic, and requested the Secretary-General to provide consolidated information regarding ICT spending. The Assembly also endorsed the recommendation of the Advisory Committee that the Secretary-General provide, in the context of the budget proposal for 2022, a comprehensive plan identifying ICT initiatives implemented in recent years and projects that would be required in the near future, along with the respective costs, estimated requirements and any expected efficiency gains (A/75/7, para. XI.19).

4. While considering the resource proposals for 2023 under section 29C, Office of Information and Communications Technology, the Advisory Committee also observed in paragraph VIII.62 of its first report on the proposed budget for 2022 (A/76/7) that, upon enquiry, it had been informed that a capital investment plan was under development to support the replacement of outdated equipment and systems and the concomitant enhancement of capabilities to meet current requirements and comply with industry and accessibility standards. The plan would put forward proposals related to the capital investment programme for ICT operations, including for conferencing equipment, and would provide detailed information on Secretariat-wide ICT operations and initiatives in the context of the proposed programme budget for 2023. While noting that a capital investment plan was under development and would be presented to the General Assembly during its seventy-seventh session, the Committee stressed the importance of providing comprehensive, detailed, transparent and accurate information on ICT resources and costs across all funding sources.

5. In addition, in paragraph XI.26 of that report, in relation to its review of the United Nations enterprise network, the Advisory Committee also noted the ongoing assessment of ICT capital expenditures globally, and that the outcome thereof would be reported to the General Assembly during its seventy-seventh session.

6. Furthermore, in paragraph VIII.56, in relation to resources for furniture and equipment under section 29C, the Advisory Committee noted that equipment was being operated beyond its life expectancy, posing a risk to information security and network resilience. The General Assembly endorsed the recommendation of the Committee that the Secretary-General provide consolidated information on the status of upgrading of obsolete ICT equipment in the forthcoming capital investment plan and that the Secretary-General should provide disaggregated information for ICT components and other elements under the furniture and equipment budget class, with a view to enhancing transparency in the presentation of ICT resources.

7. The present report seeks to respond to the above recommendations incrementally by first providing comprehensive information on ICT spending globally, including important information and trends about the value of ICT assets, equipment and inventory.

8. Expenditure information in Umoja is captured under funds centres relating to different entities (departments, offices, special political missions, peacekeeping missions, tribunals, etc.). Expenditure is also recorded using product IDs, which are categorized according to the United Nations Standard Products and Services Code and then assigned to commitment items depending on the nature of the item procured. Such commitment items are then grouped under budget classes or commitment groups, based on the type of budget (regular budget, peacekeeping budget, etc.).

9. In order to get as comprehensive a picture of ICT spending as possible, the expenditure in Umoja has been analysed for the period from January 2017 to July 2022, using a combination of information about ICT commitment items, funds centres of entities that are ICT service providers or major users of ICT, vendors that typically provide ICT goods and services, the costs of personnel who have job titles associated with the Information and Telecommunications Technology Network, and so on. For this analysis, information management positions were excluded, despite their falling within this job network, as the nature of their functions may entail responsibilities that fall outside the scope of the present report. Owing to this conservative approach, the actual ICT spending for personnel is therefore likely higher than what is indicated herein.

10. The analysis shows Secretariat-wide ICT spending by object of expenditure during the period from January 2017 through July 2022, based on the data available in Umoja (see table 1). The spending on personnel who, based on their job titles and job networks, perform ICT functions, even though they do not reside within traditional ICT service providers of the Organization, is also included separately in the table. As seen in the table, total global ICT expenditure in 2021 amounted to around \$784 million. The annual ICT spending from 2017 to 2021 was \$773 million on average.

#### Table 1

## Information and communications technology spending by object of expenditure, 2017–2022

(Millions of United States dollars)

Object of expenditure	2017	2018	2019	2020	2021	2022 (1 January to 31 July)
Posts	199.0	194.7	186.2	186.3	187.3	107.7
Other staff costs	28.5	29.2	28.5	24.3	27.3	16.3
Consultants and experts	2.8	3.8	2.7	3.1	4.1	2.4
Travel of staff	3.4	3.0	2.8	0.4	0.9	1.2
Contractual services	185.2	161.7	193.0	188.4	182.2	108.6
General operating expenses	153.4	151.6	131.5	141.8	120.4	94.2
Furniture and equipment	114.8	108.3	142.4	138.5	167.3	86.0

Object of expenditure	2017	2018	2019	2020	2021	2022 (1 January to 31 July)
Grants and contributions	7.2	1.6	4.9	2.0	1.7	0.4
Supplies and materials	13.9	21.9	34.8	11.6	18.1	7.8
Other costs	13.7	13.3	13.1	12.7	13.2	7.3
Subtotal	722.1	689.2	739.9	708.9	722.5	432.0
Posts and other staff costs (in non-ICT funds centres)	50.3	52.5	55.7	60.1	61.4	35.3
Total	772.3	741.8	795.7	769.0	783.9	467.3

11. Posts and other staff costs cover staff performing ICT functions as part of traditional ICT service providers. Such spending, on average, constituted 28 per cent of the total ICT spending during the period 2017–2021.

12. Posts and other staff costs pertaining to positions with job titles within the Information and Telecommunication Technology Network but outside traditional ICT service providers averaged \$56 million during the 2017–2021 period and have shown a steady increase, exceeding \$61 million in 2021. This group, on average, constituted 7 per cent of total ICT spending during 2017–2021. It should be noted, however, that there is a chance that some personnel in this group may be performing functions outside the Information and Telecommunication Technology Network. On the other hand, there may be other positions throughout the Organization which may be performing ICT functions but are not captured in this analysis because their job titles do not fall within this job network.

13. The costs under contractual services predominantly relate to the costs of personnel who provide or support ICT services. There are three major providers: two United Nations system entities and one commercial vendor. Spending on contractual services constituted, on average, 24 per cent of total ICT spending during 2017–2021.

14. General operating expenses include communication carrier services (51 per cent), communication maintenance (35 per cent), rental of ICT equipment (5 per cent) and other miscellaneous services (7 per cent). Spending under this category constituted, on average, 18 per cent of the overall ICT spending during 2017–2021. During the same five-year period, \$126.5 million under this category constituted payments to the same three major service providers, highlighted under contractual services, whose personnel provide or support ICT services.

15. Thus, the overall spending on personnel, including staff, contractors and consultants, made up, on average, some 63 per cent of total ICT spending during 2017–2021. In 2021, overall spending on such personnel amounted to around \$481 million, out of a total of \$784 million.

16. The furniture and equipment category covers mainly spending on communications and network equipment, audiovisual equipment, printing equipment, software, licences and office equipment. During the period 2017–2021, on average, 17 per cent of ICT spending was in this category.

17. ICT spending under supplies and materials relates predominantly to spare parts for communications networks and end-user equipment, and storage. This category constituted an average of 3 per cent of the spending during 2017–2021.

18. Table 2 shows the Secretariat-wide ICT spending by budget part and section during the period 2017–2022. The table aggregates expenditure across all funds and financial statement volumes to provide a holistic picture of ICT spending across all funding sources and types. For example, section 5, Peacekeeping operations, would

include expenditure funded from the regular budget, such as the United Nations Military Observer Group in India and Pakistan and the United Nations Truce Supervision Organization, combined with peacekeeping missions funded from their respective funds. The table also shows ICT expenditure funded from income-producing activities as well as those relating to the tribunals.

### Table 2

### Information and communications technology spending by thematic area, 2017–2022

(Millions of United States dollars)

		2017	2018	2019	2020	2021	2022 (1 January to 31 July)
I.	Overall policymaking, direction and coordination						
1.	Overall policymaking, direction and coordination	1.5	0.5	3.6	4.6	6.1	1.5
2.	General Assembly and Economic and Social Council affairs and conference management	12.4	12.1	18.4	16.5	16.2	11.5
	Subtotal	13.9	12.6	22.1	21.1	22.3	13.0
II.	Political affairs						
3.	Political affairs	49.1	39.5	66.2	41.0	37.3	28.5
4.	Disarmament	0.5	0.4	0.3	0.5	0.4	0.4
5.	Peacekeeping operations	411.4	413.9	364.1	351.9	336.3	220.8
6.	Peaceful uses of outer space	0.0	0.1	0.1	0.1	0.1	0.1
	Subtotal	461.1	453.8	430.7	393.4	374.0	249.8
Ш	.International justice and law						
7.	International Court of Justice	1.3	1.0	1.0	1.1	1.0	0.9
8.	Legal affairs	2.0	1.8	2.3	8.7	2.8	4.1
	Subtotal	3.3	2.7	3.3	9.8	3.9	5.0
IV.	International cooperation for development						
9.	Economic and social affairs	5.6	4.4	4.8	5.4	6.2	2.6
10.	Least developed countries, landlocked developing countries and small island developing States	0.0	0.0	0.0	0.0	0.0	0.0
11.	United Nations support for the New Partnership for Africa's Development	0.0	0.0	0.0	0.1	0.1	0.0
12.	Trade and development	9.9	10.8	11.5	13.7	14.1	7.8
14.	Environment	7.4	7.7	8.2	7.4	9.3	5.5
15.	Human settlements	2.3	3.1	2.9	2.0	1.9	1.4
16.	International drug control, crime and terrorism prevention and criminal justice	16.3	16.9	15.3	18.6	21.2	9.8
	Subtotal	41.5	43.0	42.7	47.2	52.7	27.1
V.	Regional cooperation for development						
18.	Economic and social development in Africa	11.4	8.2	13.5	10.4	15.8	6.7
19.	Economic and social development in Asia and the Pacific	4.5	3.9	4.7	5.9	6.0	2.5
20.	Economic development in Europe	4.0	3.2	3.6	3.2	3.1	1.7
21.	Economic and social development in Latin America and the Caribbean	9.0	8.1	9.2	8.4	8.4	4.5

	2017	2018	2019	2020	2021	2022 (1 January to 31 July)
22. Economic and social development in Western Asia	3.1	2.7	3.0	3.3	5.8	3.0
23. Regular programme of technical cooperation	0.6	0.3	0.3	0.8	0.9	0.6
Subtotal	32.7	26.5	34.3	32.0	40.0	18.9
VI. Human rights and humanitarian affairs						
24. Human rights	9.4	10.7	10.2	12.6	10.3	7.5
27. Humanitarian assistance	14.9	14.8	13.6	16.2	13.2	8.2
Subtotal	24.3	25.5	23.8	28.8	23.6	15.7
VII. Public information						
28. Global communications	3.5	4.0	4.2	7.2	9.9	4.6
Subtotal	3.5	4.0	4.2	7.2	9.9	4.6
VIII. Common support services						
29A. Department of Management Strategy, Policy						
and Compliance	43.1	48.9	29.9	31.5	25.7	11.7
29B. Department of Operational Support	2.6	3.3	12.4	9.3	10.3	8.0
29C. Office of Information and Communications Technology	94.3	78.5	134.2	138.4	159.8	85.6
29E. Administration, Geneva	19.7	17.4	20.8	20.2	25.1	12.5
29F. Administration, Vienna	7.6	6.2	6.3	6.0	6.2	3.2
29G. Administration, Nairobi	5.8	6.0	5.8	5.6	6.0	3.2
Subtotal	173.0	160.3	209.5	211.0	233.1	124.2
IX. Internal oversight						
30. Internal oversight	0.6	0.6	0.8	0.6	0.5	0.4
Subtotal	0.6	0.6	0.8	0.6	0.5	0.4
X. Jointly financed and special expenses						
31. Jointly financed administrative activities	0.1	0.0	0.0	0.0	0.0	0.0
Subtotal	0.1	0.0	0.0	0.0	0.0	0.0
XI. Capital expenditures						
33. Construction, alteration, improvement and major						
maintenance	11.1	7.2	14.4	6.4	14.3	4.8
Subtotal	11.1	7.2	14.4	6.4	14.3	4.8
XII. Safety and security						
34. Safety and security	2.3	0.8	1.0	1.4	1.1	0.4
Subtotal	2.3	0.8	1.0	1.4	1.1	0.4
Tribunals	4.5	4.4	8.6	9.4	7.6	3.1
Income-producing activities	0.5	0.3	0.4	0.6	0.6	0.3
Other	0.0	0.1	0.1	0.1	0.1	0.0
Total	772.3	741.8	795.7	769.0	783.9	467.3

19. Peacekeeping operations accounted for, on average, 48 per cent of the total, with a downward trend over time, followed by common support services for an average of 26 per cent, with a slight upward trend in recent years.

20. The majority of ICT spending was incurred by entities included in volume II of the financial reports and audited financial statements of the United Nations (peacekeeping missions, the United Nation Global Service Centre, the Regional Service Centre in Entebbe, Uganda, and the support account for peacekeeping operations) during the period 2017–2021, making up, on average, 54 per cent of total spending. Average ICT spending by volume I entities constituted 42 per cent during the period. The United Nations Environment Programme, the United Nations Human Settlements Programme (UN-Habitat), the United Nations Office on Drugs and Crime and the tribunals together accounted for about 4 per cent, on average.

21. The bulk of ICT spending was funded by assessed sources, making up, on average, 74 per cent of the total spending during the period 2017–2021. However, the share of assessed funding decreased over time, dropping to 67 per cent in 2021. In contrast, the share of non-assessed sources increased over time, reaching 33 per cent in 2021 (see table 3).

#### Table 3

**Information and communications technology spending by funding source, 2017–2022** (Millions of United States dollars)

Total	772.3	741.8	795.7	769.0	783.9	467.3
Non-assessed <sup>a</sup>	177.5	172.5	195.9	203.3	255.0	129.4
Assessed	594.8	569.3	599.7	565.7	528.9	337.9
	2017	2018	2019	2020	2021	2022 (1 January to 31 July)

<sup>a</sup> Includes voluntary contributions, programme support and cost-recovery funding.

### Information and communications technology assets, equipment and inventory

22. ICT items are categorized in Umoja in different ways depending on their purpose and value. For financial accounting purposes, they are classified as assets (capitalized as non-current assets for items above a certain value threshold, and depreciated over their useful life), inventory (a current asset held for later use) or equipment (expensed when first used, even though they may be used for several years), as shown in the figure below.

### Accounting for assets, equipment and inventory

Assets (capitalized)	Equipment (expensed)	In	Inventory (capitalized)			
Equipment above threshold	Equipment below threshold Ron-seria	ized nt Spare parts	Consumables	Raw materials		

*Note*: For strategic deployment stocks, equipment below the threshold is considered inventory and is therefore capitalized.

23. For this analysis, the capitalized and non-capitalized items outlined above are examined holistically and referred to as equipment, as the objective is to establish a baseline for ICT equipment holdings regardless of their capitalization treatment.

24. Under the United Nations policy framework for International Public Sector Accounting Standards (IPSAS), dated December 2016, the estimated useful life for equipment categories within the scope of the present analysis is set out in table 4, based on a reasonably harmonized approach across the United Nations system.

## Table 4 International Public Sector Accounting Standards useful life

Category	Estimated useful life (years)
Audiovisual equipment	7
Communication and communications network equipment	7
Infrastructure assets - telecommunications	Variable
Information technology computer, network and storage equipment	4
Information technology end-user equipment	4

25. For fixed assets, depreciation is charged on a straight-line (linear) basis over the useful life relevant to the class of asset (outlined in table 4). The Secretariat is currently assessing the useful lives of these items in accordance with observations made by the Board of Auditors, as actual useful life tends to be longer, resulting in assets still in use despite being fully depreciated.

26. In accordance with IPSAS, the gross values for fixed assets and inventory include a standard percentage for associated costs, added automatically in Umoja, to arrive at the final cost of the items. These costs represent all costs, such as freight, insurance and import duties, to bring the items to the final location for use. These standard associated cost rates are reviewed regularly and differ from location to location. Taking these costs into consideration is relevant when assessing the realistic cost of replacing these items and bringing them into operation. The net book value of assets is the gross value reduced by depreciation; this value would also be affected by upgrades and impairments.

27. The analysis of the value of ICT equipment is hampered in part by the difference in the level of detail available in Umoja and Galileo, the latter being the asset management system used in peacekeeping operations until their migration to Umoja in 2016 and 2017. The equipment records generated in Umoja through the standard procurement, receiving and inspection processes facilitate a broader and more accurate analysis of trends in the acquisition, operation and disposal of equipment required for the successful operation of the Organization. The quality of data will improve with the passage of time as older equipment, whose information was recorded in Galileo and converted to Umoja, is retired.

28. For purposes of comparability and the provision of more realistic idea of the cost of replacing all ICT equipment, regardless of their financial treatment in the context of the financial statements, the equipment below the threshold and non-serialized equipment have been presented on the same basis as fixed assets in terms of inclusion of associated costs, based on the standard associated cost rates and the application of the same useful life standards.

### Trend analysis 2017–2022

29. A high-level analysis of trends for ICT assets, equipment and inventory for the period 2017–2022 forms the first step in gaining a better understanding of the nature and the level of investments made by the Organization in ICT equipment and the underlying organizational behaviours and structures that underpin these investments. This information will help steer further analysis of the underlying patterns and their drivers and aid in defining a baseline from which future requirements can be projected or formulated.

30. Table 5 shows the gross and net book value of all ICT equipment (assets, equipment and inventory) at the end of each year and at the end of July 2022.

### Table 5

Gross and net values of information and communications technology equipment (assets, equipment and inventory)

	Gross value (millions of United States dollars)	Net value (millions of United States dollars)	Ratio: net/gross (percentage)
31 December 2017	949.2	333.6	35
31 December 2018	971.6	305.2	31
31 December 2019	929.0	269.6	29
31 December 2020	912.3	253.4	28
31 December 2021	902.5	247.6	27
31 July 2022	886.7	246.2	28

31. Both the gross and net values of ICT equipment declined during the period from January 2017 through July 2022. The decrease could be attributed to multiple factors, such as the liquidations of missions and changes in operational strategy, among others. While the ratio of net to gross value had been relatively stable for the past four years, it declined from 35 per cent at the end of 2017 to 28 per cent by July 2022, suggesting that equipment is getting older and less valuable.

32. Disaggregating these values by peacekeeping and other operations shows that the declining trend is common to both, but the decline is more pronounced in the case of peacekeeping operations, with the ratio dropping from 37 per cent to 28 per cent, while other operations have declined only from 31 per cent to 27 per cent, as shown in table 6.

### Table 6

### Gross and net values of information and communications technology equipment (assets, equipment and inventory), by type of operation

	Gross value (millions of United States dollars)	Net value (millions of United States dollars)	Ratio: net/gross (percentage)
Non-peacekeeping (	including tribunals)		
31 December 2017	296.1	93.0	31
31 December 2018	308.1	88.4	29
31 December 2019	315.5	79.4	25
31 December 2020	328.9	80.5	24
31 December 2021	351.7	92.5	26
31 July 2022	359.1	97.0	27
Peacekeeping			
31 December 2017	652.6	240.6	37
31 December 2018	663.5	216.8	33
31 December 2019	613.5	190.2	31
31 December 2020	583.4	172.9	30
31 December 2021	550.7	155.2	28
31 July 2022	527.7	149.3	28

33. The steady decline in the ratio for peacekeeping operations could suggest that the trend may continue unless the underlying reasons are diagnosed and addressed. Relying on an ageing equipment base may not only expose the Organization to a higher risk of system failures, but it may also create pressure for larger investments to bring the equipment base back to a level that supports reliable and adequate ICT services. On the other hand, the ratio for non-peacekeeping operations has been increasing gradually since 2020. However, this does not rule out areas of high proportions of aged equipment that will have to be identified through more detailed analysis.

#### Characteristics of existing information and communications technology equipment

34. Table 7 provides an overview of the distribution of ICT equipment across the Organization on the basis of the net book value. This distribution has been derived based on who owns and uses ICT equipment. Such ownership will not necessarily correspond to how the equipment values are reported in the financial statements. For example, support account-funded equipment for Headquarters departments will still be shown under other operations, while equipment funded from peacekeeping trust funds listed in volume I of the financial reports and audited financial statements of the United Nations will be shown under the respective peacekeeping mission. This is due to the fact that the Organization's fund accounting allows for sharing across organizational boundaries and even across financial reporting volumes. Table 7 reflects the net book values on the basis of who owns the equipment.

#### Table 7

## Net book value of information and communications technology assets, inventory and equipment by operation, 2017–2022

(Millions of United States dollars)

Total	333.6	305.2	269.6	253.4	247.7	246.3
Other operations	89.1	86.0	76.6	75.3	87.7	92.7
Tribunals	3.9	2.4	2.8	5.2	4.8	4.3
Peacekeeping operations	240.6	216.8	190.2	172.9	155.2	149.3
	2017	2018	2019	2020	2021	2022 (1 January to 31 July)

35. Table 7 clearly reflects that peacekeeping operations accounted for the majority of the equipment throughout the period, followed by other operations, while the tribunals accounted for a very small portion. However, the proportion attributable to peacekeeping declined from 72 per cent in 2017 to 61 per cent at the end of July 2022, owing mainly to the reductions in the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo, the United Nations Support Office in Somalia, the African Union-United Nations Hybrid Operation in Darfur and the United Nations Global Service Centre. While reductions resulting from the closure or downsizing of missions are easy to identify, other shifts may require more detailed analysis to understand the basis for the trends. While the tribunals have increased only marginally, from 1 to 2 per cent, other operations have increased from 27 per cent in 2017 to 38 per cent at the end of July 2022.

36. In addition to the ownership of the equipment, the composition of the equipment and their associated net book values have been further disaggregated to reflect the nature of the equipment and discern any trends in the movements of their value during the period under review. The net book values are presented under the following broad categories, consistent with the classification of ICT assets for the financial statements.

### Table 8

## Net book value of information and communications technology assets, inventory and equipment by category, 2017–2022

(Millions of United States dollars)

	2017	2018	2019	2020	2021	2022 (1 January to 31 July)
Audiovisual equipment	17.3	14.7	11.9	12.1	14.2	16.3
Communication and communications network equipment	143.5	132.7	119.8	108.2	102.8	96.1
Infrastructure assets - telecommunications	13.8	13.7	11.9	10.0	6.6	5.8
Information technology computer, network and storage equipment	92.4	81.2	75.0	67.3	64.1	65.1
Information technology end-user equipment	66.4	62.9	50.9	55.8	60.0	63.0
Total	333.6	305.2	269.6	253.4	247.6	246.2

37. As at 31 July 2022, communication and communications network equipment accounted for 39 per cent of the total net book value for ICT assets, inventory and equipment. Within this category, 62 per cent related to fixed network equipment such as antennas and towers, satellite equipment, communication shelters and radio equipment, followed by 17 per cent for videoconferencing equipment. In comparison, 77 per cent of the total net book value related to fixed network equipment and 12 per cent to videoconferencing equipment in 2017, which seems to illustrate a gradual shift in the composition of the within-category equipment composition.

38. The information technology computer, network and storage equipment category accounts for 26 per cent of the total net book value for ICT assets, inventory and equipment as at 31 July 2022. Similar to the previous category, though it is less pronounced, there has been a gradual reduction in the proportion of this equipment category compared with the other four categories, from 28 per cent in 2017 to 26 per cent as at 31 July 2022. This category consists mainly of network service equipment (52 per cent), which includes switches, routers and wireless access points, followed by computer servers (14 per cent), network security equipment (8 per cent) and network installation equipment (5 per cent).

39. The net book value for network service equipment, computer servers and, to a lesser extent, network installation equipment has been declining since 2017, while there has been a small increase in network security equipment from 2019 to 2021, followed by a decrease as at 31 July 2022.

40. Information technology end-user equipment consists of predominantly notebook computers. The values of tablets and of desktop computers are nearly equal to each other, but are much lower in value than notebook computers. Notebook computers and tablets are gradually replacing desktop computers. Printers and monitors also constitute a major category, similar to desktop computers. The net book value for equipment in this category has been increasing steadily for the past four years.

### Ageing of information and communications technology equipment

41. The declining net book values across all equipment categories and departmental groups over the five-year period likely reflect the effects of multiple factors. While some of these factors may indicate developments such as the liquidation of peacekeeping missions and other positive strategic shifts towards less hardware-

intensive operations or more affordable technology, the ratio seems to indicate that the equipment pool is becoming increasingly aged.

42. A review of the proportions of active equipment that are within and beyond their anticipated useful lives over the period 2017–2021 indicates that the level of equipment that is being utilized beyond its useful life increased from 17 per cent in 2017 to 30 per cent in 2021. While this trend is prevalent in both peacekeeping and other operations, the increase in the level is more prominent outside peacekeeping operations. Similarly, when examining the average actual years in use across the different equipment categories, they reflect an upward trend for the majority of the categories. This seems to suggest that not only is the Organization reliant on equipment that is increasingly operating beyond its useful life, but the equipment is also being retained for use for longer periods after reaching the end of its useful life.

43. As reliance on an increasingly ageing equipment base can have a serious detrimental impact on the operations of the Organization, it is crucial that these trends be examined further to establish the underlying drivers, so that mitigating measures can be identified as soon as possible to reverse this negative trend.

44. As indicated earlier, currently, the useful life of equipment is established on the basis of the United Nations policy framework for IPSAS. While these values can be used to provide a useful indicator when examining any shifts in the ageing of equipment, it is also important to note that the operational life of ICT equipment is usually greater than the IPSAS useful life. As the operational useful life of equipment is affected by its operating environment and varies from location to location, it is not realistic to establish standards that can be applied uniformly across all locations.

45. For ICT equipment, some of these environmental factors include temperature and humidity levels, power fluctuations and reliability, dust, and transportation, among others. While measures are taken to control such factors and to mitigate their impact on the operational lifespan of the equipment, such as in data centres, it is not feasible to fully eradicate their impact. Equipment located outside these controlled environments, especially end-user equipment, is more prone to be affected by these environmental factors.

46. Establishing the operational life, which would give a more accurate picture of the lifespan of the equipment, requires a more detailed analysis of the environmental factors described above and their effect on the lifespan of the various equipment types at the location level. Even though operational depreciation scales have been established for groups of equipment, they do not include location-specific factors.

47. A global ICT equipment replacement plan would require a detailed analysis of the status of equipment in each entity, considering factors such as the availability of support for equipment in use and technological upgrades, as well as global United Nations standards. The financing for such replacements would then have to be analysed with reference to the funding gap, if any, of the entity's ICT budget. In summary, therefore, while this analysis provides interesting and valuable information, it is inconclusive with regard to the urgency of, or need for, additional funding beyond that currently being budgeted on a recurring or periodic basis. However, the high depreciation and extended use of ICT equipment beyond its useful life point to the need for a disaggregated review of equipment needs and their replacement plans.

### Information and communications technology applications

48. ICT applications cover a broad spectrum of software, ranging from those essential for computers to operate to others required for business purposes. Like most organizations, the United Nations has a large portfolio of business solutions which include off-the-shelf, customized and/or internally developed software. Only a

handful of these solutions meet the threshold for being recorded and tracked in the Organization's systems as intangible assets. A preliminary review of this information shows that it would not be very useful in making a determination of the investment needs for their enhancement or replacement. While the Office of Information and Communications Technology has prescribed a system for tracking applications, some of the information is not mandatory and, therefore, the data in this system is not robust enough to draw conclusions about the cost of such systems or the investments that would be needed for their upkeep or replacement.

49. The ICT governance process requires new systems to be vetted and cleared before investment decisions are made. Proposals for new systems or replacements for existing systems should therefore be guided by approvals through the current governance process. No inventory of such approved proposals is currently available. They will be presented in future capital investment proposals when they become available.

50. The Department for General Assembly and Conference Management is currently responsible for a wide range of applications that support conferencing and event management, and other aspects of its work. The Department is currently evaluating the architecture and functionality of these applications in order to improve the processes that they support. It is not clear yet whether these systems will need any additional funding beyond that already budgeted.

51. Funding for the enhancement or replacement of enterprise systems such as the un.org domain name, Inspira, Umoja, iNeed, iSeek and email, among others, will also go through the ICT governance process before such proposals are presented for additional financing.

# III. Reinforcement of the global cyberprotection of the Secretariat

52. As noted in General Assembly resolution 73/27 on developments in the field of information and telecommunications in the context of international security and resolution 73/266 on advancing responsible State behaviour in cyberspace in the context of international security, in today's digitalized world, cybersecurity has emerged as a matter of critical importance.

53. Dependence on ICT and cyberenabled solutions has led to an unprecedented increase in cybersecurity risks and threats, which are constantly growing in sophistication and disruptive potential, including beyond ICT areas, such as in connection with the protection of the financial, legal and reputational interests of an organization.

54. In this context, the Joint Inspection Unit, in its report of October 2021 (JIU/REP/2021/3), noted that the increased damaging potential of the cybersecurity risk map required a focused effort and that the Secretary-General should present a report to the General Assembly no later than at its seventy-eighth session, exploring opportunities for the convergence between physical security and cybersecurity to ensure a holistic protection of personnel and assets, indicating measures to strengthen structures accordingly.

55. The Advisory Committee also addressed cybersecurity during its review of the programme budget for 2022. In paragraph VIII.63 of its report (A/76/7), the Committee reiterated that the next ICT strategy should pay heightened attention to information security and provide a comprehensive action plan identifying ongoing and future initiatives and their expected benefits, risks and costs, with time-bound objectives, clear benchmarks and compliance mechanisms. The Committee also recommended that

the Secretary-General should provide updated information on the implementation of the ongoing and planned cybersecurity measures, as well as their effectiveness in preventing and responding to cyberattacks, in the context of the next budget submission. The General Assembly endorsed the Committee's recommendations.

56. Explicitly determined in the Joint Inspection Unit report are the following four areas to reinforce capabilities for cyberprotection:

(a) Building on the convergence between physical security and cybersecurity systems;

- (b) Optimizing resource allocation for cybersecurity;
- (c) Expanding in-house expertise;
- (d) Investing in technology for cybersecurity.

57. In response to the General Assembly's request, the Office of Information and Communications Technology and the Office of Programme Planning, Finance and Budget conducted an assessment to identify the requirements to cover the widened scope of work and expanded scale of coverage that would be required to protect the global Secretariat against the expanded cybersecurity risk map.

58. The starting point of the exercise was to determine the coverage of the current cybersecurity programme across the Secretariat in relation to the four areas set out in the Joint Inspection Unit report. The assessment included an additional benchmarking review of prevailing industry best practices, since the cybersecurity risk map facing the Organization is not different in complexity or scope relative to those facing other global organizations in the public or private sector.

59. Also considered in the assessment was the growing use of new ICT-dependent methods of work and new modalities for servicing conferences and meetings following the COVID-19 pandemic, which, in turn, has expanded and deepened reliance on and the complexity of implementation of the underlying suite of ICT operations to support the new services.

60. The present report provides an outline of the outcomes of the assessment, with related proposals formulated by the Office of Information and Communications Technology to urgently initiate a reinforcement of capabilities for the global cyberprotection of the Organization, as requested by the General Assembly.

61. The assessment, including the benchmarking, highlighted the following main gaps and suboptimal aspects to be addressed:

(a) The ICT policy framework does not establish a clear matrix of roles and authority for cybersecurity mapped across the federated ICT model;

(b) The ICT policy framework does not prescribe authority to vet configuration baselines and operating procedures for technologies and platforms;

(c) New skills are required to deliver effective cybersecurity, in particular concerning cutting-edge technology (vulnerability assessment, automated response, etc.);

(d) There is limited internal ability to design and architect solutions for areas beyond traditional ICT, such as facility, security and conference systems;

(e) There are limited technological capabilities, tooling and software through which to quickly ensure disaster recovery and business continuity.

62. These factors and the heightened threats pointed to the need for a holistic transformation of the ICT policy framework and federated operations, specifically by implementing the following:

(a) A widened scope of cybersecurity work (additional work streams);

(b) An expanded scale of coverage (additional capacity across the Organization);

(c) Deployment of additional technology for cybersecurity.

63. The assessment, including the benchmarking described above, highlighted the urgent need of the Office of Information and Communications Technology to restructure its programme of work for cybersecurity, along with a reorganization of the division of labour across the global Secretariat. The reorganization is required to enable effective servicing of all the work streams under which modern cybersecurity is organized.

64. As the benchmarking exercise demonstrated, a modern programme of work for cybersecurity is typically structured across the following four major areas of work, with distinct portfolios of duties and skill sets both for specialization and segregation for internal controls:

(a) **Governance:** this work stream has to update the global cybersecurity framework of the Secretariat, covering the further development of ICT policies and standards with the related operating procedures and protocols to respond to the expanded and evolved sophistication of the cybersecurity risk map. This revised framework will determine the mapping of work and responsibilities for cybersecurity across the Secretariat to ensure compliance and establish a clear division of labour between the global roles of the Office of Information and Communications Technology on the one hand and the operational work delivered by the local ICT units by alignment with the Office-established policy framework on the other hand. This work stream has to be driven by the Office in accordance with its central authority for ICT across the Secretariat;

(b) **Prevention:** this work stream would focus on the systematic mapping of activities across the ICT landscape to reduce the potential for cybersecurity risks, including patch and vulnerability management; vulnerability assessments; issuance of security advisories and compliance tracking; establishment of security baselines; network segmentation; identity and access management; disaster recovery and resilience (business continuity); malware protection; data protection and privacy; data loss prevention; and application security. This area needs additional specialized capacity in the Office;

(c) **Detection:** this work stream would cover practices and activities focused on prognosis of possible and timely detection of cybersecurity risks, including stateof-the-art threat detection engineering; assessment of application security for cybersecurity risks; threat-hunting tools; integrated security monitoring; cyberthreat intelligence; reputation protection operating protocols; and application- and cloudspecific assessments and controls. This area of work and team would be the one delivering comprehensive cybersecurity assessments (red team exercises), as and when required. This area would need significant capacity reinforcement in the Office;

(d) **Response and associated operational services:** this work stream covers operational activities to execute whenever cybersecurity incidents are detected, including timely reporting with indication of magnitude, to promptly respond in a coordinated way to limit damage and reduce recovery time. This area needs select capacity reinforcement across the Secretariat.

65. As described above, the reinforcement of the capacity of the Office of Information and Communications Technology to cover the widened scope of the cybersecurity programme of work will also require an expanded scale of coverage across the established offices of the Secretariat. The reinforcement of the cybersecurity protection of the global Secretariat will require three complementing reinforcements: (a) additional staff positions to increase internal capacity to cover the widened scope of work and minimize dependency on costlier external contractors; (b) distributing the increased staffing capacity across duty stations to cover the expanded scale of coverage; and (c) expanded technological capability for the Organization.

66. The Cybersecurity Service of the Office of Information and Communications Technology currently has 14 staff and 16 contractors covering the limited scope of current work streams globally. These comprise 11 staff in New York and 3 staff covering Nairobi, Bangkok and Geneva. The contractors are distributed as seven in New York, eight in Valencia and one in Brindisi.

67. The widened scope of work and expanded coverage of the Secretariat locations will require 12 new posts (1 P-5, 5 P-4, 4 P-3 and 2 P-2) and 6 new general temporary assistance positions (3 P-2 and 3 General Service (Principal level)), all in the Office of Information and Communications Technology. Of the 18 posts and positions, 11 will serve to establish new staffing capacity for the Office of Information and Communications Technology in Addis Ababa, Beirut, Santiago, Vienna, Valencia and Brindisi, while 7 will add staffing capacity in New York, Geneva and Nairobi, building on resources previously approved by the General Assembly for these locations. In terms of functions, 11 posts and three positions will be assigned to reinforce the scope of work of the prevention work stream, which includes global vulnerability management, threat assessment and related monitoring to support local ICT units. One post and three positions will be assigned to reinforce the capacity of the detection and incident response work streams. Three positions in New York, two in Valencia and one in Brindisi, which are meant to augment existing capacity for vulnerability management, and threat and incident management, are proposed to be general temporary assistance positions initially to allow for time to assess the effectiveness of this distribution of capacity.

68. The functional profiles of the 18 new posts and new general temporary assistance positions by category, grade level and duty station of assignment are detailed in table 9.

Duty station	Post/general temporary assistance	Grade	Functional profile of the posts and new general temporary assistance positions by office
New York	Post	P-5	To split the Office of Information and Communications Technology cybersecurity work streams (protection and detection) to enhance capacity and for internal controls by segregation of authority
Addis Ababa	Post	P-4	New Office of Information and Communications Technology
Beirut	Post	P-4	cybersecurity focal points focusing on the cyberprevention work stream, located in Addis Ababa, Beirut, Santiago and
Santiago	Post	P-4	Vienna, as the other established offices already have focal points
Vienna	Post	P-4	Point
Valencia	Post	P-4	To support global threat and incident management technology operations
Brindisi	Post	P-3	To strengthen vulnerability management capacity
Geneva	Post	P-3	To reinforce capacity in Geneva, given the volume of United Nations entities based there, and to cover Bonn, Germany
Nairobi	Post	P-3	To reinforce capacity in Nairobi, given the volume of United Nations entities based there
Valencia	Post	P-3	To support the global Secretariat operational resilience programme
Valencia	Post	P-2	To support technical security architecture and design for key initiatives
New York	Post	P-2	To reinforce security architecture and design support for projects
New York	GTA	P-2	To increase capacity for the threat and incident management function in New York
New York	GTA	P-2	To strengthen capacity for vulnerability management in New
New York	GTA	P-2	York and Brindisi
Brindisi	GTA	GS (PL)	
Valencia	GTA	GS (PL)	To increase capacity for threat and incident management in
Valencia	GTA	GS (PL)	Valencia

## Table 9Functional profiles by category, grade level and duty station

Abbreviations: GS (PL), General Service (Principal level); GTA, general temporary assistance.

69. As mentioned earlier, the assessment and benchmarking also highlighted the need for additional technology to support the Secretariat's cybersecurity programme. Specifically, the plan for 2023–2028, coinciding with the ICT strategy, would include the reinforcement of current capabilities with additional software, including for increased licensing for the security portfolio, and specialized tooling to increase capacity for cyberthreat detection, prevention and forensics, such as the following:

- Vulnerability scanning and application security
- · Identity and access management for cloud and on-premises systems
- Threat-hunting solution and forensic tools
- Automated capabilities to assess development code and configuration baselines for systems
- Specialized cross-cutting technical solutions to converge across systems beyond information technology specifics (security, building, videoconferencing, etc.)
- Enterprise-grade forensic technology, including for cloud hosting

70. The exact technology architecture and portfolio for the cybersecurity programme covering 2024-2028 will be determined in 2023 following a comprehensive assessment of needs-driven identification of suitable technological solutions and road maps across the various commercial options for cybersecurity technology, which will include considerations of suitability and interoperability. These will be addressed holistically and in greater detail with an implementation road map in a report that is proposed to be submitted to the General Assembly at its seventy-eighth session. This comprehensive report on the global upgrade of capabilities for cybersecurity, further to the outline presented in the present initial report, would spell out the technology road map and the functional activities of the various resource components by work stream area, unit and duty station, including resources already available, interlinking the plan with the existing budgets across all funding sources and determining the coordination and division of labour across ICT units, including the United Nations Global Service Centre, to optimize synergies and avoid duplication, as requested by the Assembly. The report will also link the cybersecurity technology road map and related investment plans with the rest of the ICT strategy and the technology road map.

71. In order to quickly and proactively enhance the Secretariat's cyberprotection capabilities in the face of growing threats, the Secretariat would need to commission urgently, during 2023, an assessment by a specialized company to help the Office of Information and Communications Technology to complete a comprehensive road map for the Secretariat's cybersecurity capacity and reorganization plan for 2024–2028. This will also facilitate the finalization of the assessment of the portfolio of technology solutions for cybersecurity, including software options suited for the Secretariat's ICT architecture and evolving needs. Accordingly, the Secretary-General proposes an additional \$400,000 for contractual services under the proposed programme budget of the Office of Information and Communications Technology for 2023.

72. Microsoft 365 Enterprise E5 security licences will provide comprehensive and globally consistent protection for users' computers, including, inter alia, for email and Internet access filtering and malware protection. Elements of these solutions were first deployed in 2021 for a limited population, while the global deployment of the comprehensive suite of solutions is continuing within existing resources by delaying other expenditure, in view of the urgency of improving the cyberprotection. For 2023, the resource requirements for the Microsoft E5 security licences would cumulatively amount to \$4,700,000. Additionally, resources amounting to \$800,000 would be required to deploy new software and tools for vulnerability management.

73. If the additional staffing capacity proposed in the present report is established, the existing pool of 16 contractors supporting cybersecurity could remain at the current level funded under the Office of Information and Communications Technology, but repurposed gradually to support: (a) implementation of specialized technology to deploy tools and allow time for internal capacity to build in relation to such new tools during the roll-out and initial phases of usage; and (b) ad hoc services for capabilities not requiring permanent capacity.

74. In view of the phased roll-out of new technologies, the 18 new posts and positions are also proposed to be established in two phases, in 2023 and 2024, subject to a 50 per cent vacancy rate in accordance with the established practice for new posts and positions. In the first phase, it is proposed to establish four posts (P-4), in Addis Ababa, Beirut, Santiago and Vienna, to add new capacity in those locations for supporting them locally, and six general temporary assistance positions (three P-2 in New York, two General Service (Principal level) in Valencia, and one General Service (Principal level) in Brindisi), to augment existing capacity. The remaining eight posts will be proposed in the budget for 2024.

#### Table 10

### Preliminary estimate of financial resources by object of expenditure

(Thousands of United States dollars)

	2023 estimate	2024 estimate <sup>a</sup>
Posts	398.5	1 429.1
Other staff costs	364.2	618.9
Consultants	_	_
Travel of staff	_	_
Contractual services	400.0	400.0
General operating expenses	5 500.0	5 500.0
Supplies and materials	_	_
Furniture and equipment	_	-
Total (net of staff assessment)	6 662.7	7 948.0

<sup>*a*</sup> The 2024 estimate is added for informational purposes only.

75. Annex I provides an overview of the gaps in the current cybersecurity programme in the Organization, indicating how the expanded capacity will cover the gaps in 2023 through 2028, as outlined in the present report.

### IV. Safety and security

76. In the context of the review of the resource proposals for section 33 of the proposed programme budget for 2022, the General Assembly had endorsed the recommendation of the Advisory Committee in paragraph XI.27 of its report (A/76/7) that the Secretary-General provide detailed information on the scope of the required upgrades and enhancements, along with related cost implications, in the next budget submission. In addition, the Committee was informed<sup>1</sup> that the Department of Safety and Security was conducting a review of the physical security systems at headquarters locations to provide an overview of the situation, and of the scope of the upgrades and enhancements that needed to be implemented from 2023 to 2028. The Committee was also informed that the outcome of the review would be reported to the Member States in the context of the 2023 budget proposal.

77. The assessment of investment requirements to upgrade capabilities for safety and security services across the eight headquarters duty stations was undertaken by the Department of Safety and Security and the Office of Programme Planning, Finance and Budget from March to August 2022. In terms of scope, the assessment

<sup>&</sup>lt;sup>1</sup> See A/76/7, para. XII.28.

focused on the following four main areas that typically require investments, with the first two representing the bulk of requirements:

- (a) Physical security infrastructure (including equipment);
- (b) Security systems;
- (c) Safety operations;
- (d) Technical consultancies for external quality assurance.

78. The following factors are driving the urgent requirement for investment in a global upgrade of safety and security capabilities across the headquarters locations of the Secretariat:

(a) Evolved security risk map, with expanded technical sophistication of risk;

(b) The need for safety and security capabilities to grow beyond perimeter and physical security into integrated solutions to respond to the evolved risk map by systemic convergence to enable agile pre-emptive capabilities;

(c) The standardized access control system, implemented in 2011, requires upgrades to the underlying infrastructure across duty stations;

(d) Further standardization is required for perimeter protection and integrated access control with screening, detection and surveillance.

79. The assessment confirmed the importance of integrated planning for investments in safety and security services upgrades and replacements:

(a) Threats to safety and security need to be evaluated holistically, and upgrades and replacements of safety and security services equipment and systems should not be driven by the end of life cycles;

(b) Integrated systemic solutions are a key feature of modern safety and security capabilities, such as integration of access systems with enhanced imaging video for detection, screening and surveillance analytics, with linkages across alarms, barriers and gate systems;

(c) Access control needs to grow with modern technology to integrate detection, screening and surveillance. Hence, the global upgrade proposal has to include the integration of access control and the identification system across offices to establish an integrated Secretariat-wide solution;

(d) The upgrade plans have to follow a phased implementation schedule to minimize operational disruption, provide lessons learned for subsequent rounds and optimize cost-effectiveness;

(e) Holistic technical planning is required with each local ICT service, since subsystems and hardware at each office may need different upgrade and sequencing plans to ensure sustainable interoperability in the long run;

(f) Limited project management capacity for safety and security across duty stations has led to inconsistent maintenance and limited capacity to upgrade;

(g) The Department of Safety and Security will need to assign a dedicated team to produce the global upgrade plan during 2023, vetting road maps (compliance, standardization and timeline), and then to ensure oversight during the implementation phase.

80. The Department of Safety and Security assessment confirmed a total of 606 projects (grouped into 163 series) for the upgrade requirements for safety and security across the eight headquarters locations for implementation during 2024–2034, including the urgent initiation of some upgrades to be implemented at the Economic

Commission for Africa (ECA) during 2023. The preliminary estimate of requirements, for information purposes, totals \$94,385,600 over the 11-year period prior to adjustment factors, such as escalation costs, inflation, contingency or maintenance requirements.

81. Grouped under the four operational areas historically categorizing such operations, as explained in paragraph 77 of the present report, the 163 project series have been consolidated in an integration matrix determining cross-dependencies and the annualized sequence of implementation during the 11-year schedule.

82. The upgrades required by duty station and by category of investment type are outlined below.

(a) Economic Commission for Latin America and the Caribbean: the preliminary estimate of \$8,667,300 covers a total of 10 project series during 2024–2034. In addition to replacements, the Department of Safety and Security has assessed requirements against the changing environment in the Santiago area, which advise a reinforcement of access control and the upgrade of the physical security subsystems integrated through the underlying C-Cure system, along with an update of the underlying infrastructure;

(b) Economic and Social Commission for Asia and the Pacific: the preliminary estimate of \$2,607,000 covers a total of 17 project series during 2024–2034. The main objective to be addressed by the specific investment plan concerns the upgrade of access control and physical security systems and components;

(c) **Economic and Social Commission for West Asia:** the preliminary estimate of \$8,740,000 covers only eight project series during 2024–2034. The major areas to be addressed by the investment plan include two critical immediate projects: (a) integration of the access control and associated system components with the fire alarm for interoperable capabilities; and (b) anti-blast mitigation with reinforcements across the building following the protection design after the 2020 Beirut port explosion;

(d) United Nations Headquarters: the preliminary estimate of \$15,667,800 covers 22 project series for implementation during 2024–2034. The plan includes completion of safety and security features in the delegates' entrance and infrastructure upgrades for the interoperable global access control identification card;

(e) United Nations Office at Geneva: the preliminary estimate of \$14,034,000 covers seven project series during 2024–2034. The major areas to be addressed include the replacement of doors for the historical buildings to implement a layered compartmentalization of protection, the upgrade of screening and detection capabilities across campus and the reinforcement of its perimeter;

(f) United Nations Office at Nairobi: the preliminary estimate of \$10,794,100 covers 50 project series during 2024–2034. The plan includes upgrades to the safety and security infrastructure, the operations centre, the electronic firearms armoury and the upgrade of the visitors pavilion;

(g) United Nations Office at Vienna: the host country has affirmed its intention to undertake a comprehensive renovation of the Vienna International Centre. Therefore, a review of implications vis-à-vis safety and security would be possible once the comprehensive renovation plan for the Centre is available. The financing of the safety and security upgrades would also be shared among the United Nations, the International Atomic Energy Agency, the United Nations Industrial Development Organization and the Comprehensive Nuclear-Test-Ban Treaty Organization. However, a very preliminary estimate of upgrading the safety and security systems at the Centre has been established at \$18,140,000, covering 19 project series, which would have to be shared among the four entities mentioned earlier, after the projects are approved;

(h) **Economic Commission for Africa:** the preliminary estimate of \$15,735,500 covers a total of 30 project series during 2023–2034. Unlike all other headquarters locations, the assessment conducted by the Department of Safety and Security at ECA in August 2022 highlighted the need for an urgent series of upgrades, as the changed security situation in Addis Ababa has rendered the campus non-compliant with minimum operating security standards. These urgent requirements, explained separately later, relate to strengthening perimeter protection, reinforced ballistic protection and compartmentalization across buildings and pathways to mitigate risks.

83. Annex II provides a high-level overview of all the projects across duty stations and over the 11-year period 2024–2034 (and also in 2023 for ECA). Although based on very detailed work, these preliminary estimates are still subject to variance owing to inflation and contingency, among others. The figures in that annex, rounded to the nearest hundred dollars, are provided in the present report. The Secretary-General will present a comprehensive report on the global upgrade of capabilities for safety and security to the General Assembly at its seventy-eighth session, further to the outline presented in the present report.

### V. Buildings and facilities

84. At the request of the General Assembly in 2009, a strategic capital review exercise was initiated to assess investment requirements for buildings and facilities across the established offices of the Secretariat. Through assessment exercises conducted during 2010-2017, reports were presented to the Assembly during its sixty-fifth, sixty-eighth, sixty-ninth, seventieth and seventy-second sessions.<sup>2</sup>

85. Following the strategic capital reviews, the General Assembly repeatedly requested that reports on expenditure and investment proposals provide holistic, consolidated and transparent information on every component, interlinking ongoing projects and future investment plans with the related expenditure and budget information, along with justification highlighting the expected efficiency gains and benefits, to allow for effective deliberations by the Assembly.

86. In response to the General Assembly's requests, the Secretariat initiated a programme of work in 2022 to systematically identify and assess capital investment requirements across the Secretariat with an integrated scope and a mid- to long-term time frame. The initial scope was limited to United Nations Headquarters, offices away from Headquarters and four regional commissions, with a focus on four areas that have historically been the areas of interest for capital investments, namely buildings and facilities, safety and security, underlying ICT and local infrastructure to support conferencing. While reviewing these four areas, the assessment also factored in cross-implementation requirements derived from mandates prescribed by the Assembly in respect of sustainability, accessibility, business continuity, well-being, health care and standardization.

87. The assessment had three objectives: (a) to complete an initial identification of investment requirements across the eight headquarters locations through a holistic scope and a long-term vision, building on the lessons learned from the strategic capital review; (b) to establish a consistent approach and process for the systematic identification of capital investment requirements holistically across the Secretariat, to be periodically updated, to complement the current budget processes and to facilitate predictable financing of such investments that also considers cash flows and budget cycles; and (c) to establish a recurring programme of work to produce periodic

<sup>&</sup>lt;sup>2</sup> See documents A/65/351, A/68/733, A/69/760, A/70/697 and A/72/393.

reports to the General Assembly on capital investments, building on the lessons learned and baselines drawn by the current exercise.

88. The establishment of a consistent approach and process for identification of requirements was guided significantly by the lessons learned from the strategic capital review, specifically section B of the report of the Secretary-General on that topic (A/68/733), on key objectives of the global capital maintenance programme, and considered historical expenditure patterns across areas to direct the construction of the approach and templates for aggregating information.

89. A significant amount of data is being collected using a standard template that will enable analysis of multiple dimensions, such as categories of investment, office, duty station, timeline, mandated requirements such as sustainability and accessibility, and high-level dependencies within and across projects to facilitate detailed planning. The template will facilitate not only the aggregation of projects for a high-level view of the entire portfolio but also establishing parallel and serial implementation tracks, and potentially levelling financing needs, in order to adhere to General Assembly resolution 72/262, in which the Secretary-General was requested to ensure that the largest and most complex capital expenditure projects were not implemented simultaneously, in order to prevent the need to finance them at the same time.

90. Over 100 formal work meetings were scheduled across offices from March to August 2022 to develop and validate integrated plans consolidating all identified requirements by office and area in accordance with the approach described earlier. This initial assessment has highlighted the need to identify capital investments with a holistic and integrated scope to derive comprehensive assessments across a longterm financial planning cycle. It is also necessary in order to act on General Assembly requests that proposed resource requirements should be sufficiently detailed and justified, while proposals under section 33 should have greater clarity, detailed costing and transparency.

91. The assessment is striving to develop indicative estimates for information purposes on the basis of detailed information and analysis that can eventually enable the preparation of proposals for consideration by the General Assembly, including on the basis of guidance that may be provided through the intergovernmental review. The requirements are being identified and analysed by office and area to cover implementation over a 11-year financial cycle from 2024 to 2034. However, the scale and complexity of the effort suggests that an initial holistic estimate can only be developed by the Assembly at its seventy-eighth session. Such estimates are expected to cover, for each of the eight locations, requirements related to buildings and facilities, local ICT infrastructure, infrastructure for conferencing needs, and safety and security requirements. Such information is expected to be able to reflect compliance with mandates relating to accessibility, sustainability, health, safety and security and business continuity.

92. While the identification of requirements has been completed in respect of safety and security under the leadership of the Department of Safety and Security, much progress has also been made in relation to the other areas at the Economic Commission for Latin America and the Caribbean (ECLAC), the Economic and Social Commission for West Asia (ESCWA), ECA, the United Nations Office at Geneva and, to a lesser degree, the United Nations Office at Nairobi, while the United Nations Office at Vienna, the Economic and Social Commission for Asia and the Pacific, and United Nations Headquarters are likely to progress in these areas by the first quarter of 2023. For an integrated view of all the requirements, it would be important to complete the initial phase of data gathering and analysis for all the eight locations to ensure consistency in approach as well as identifying opportunities for standardization.

93. A synopsis of the assessments by location is presented below.

94. Economic Commission for Latin America and the Caribbean. The ECLAC campus in Santiago was finished in 1966. The ongoing North Building project is scheduled for completion by the end of 2023. Since 56 years have passed, some upgrade of its infrastructure is to be expected. The assessment by ECLAC of its investment needs was guided by the lessons learned from the impact of the 2010 earthquake and subsequent rebuilding and by assessing additional upgrade requirements to strengthen ECLAC infrastructure across buildings, given the permanent seismic risk of its headquarters location. The demands during the pandemic for new methods of work and modalities for servicing meetings and conferences, and increasing demand from Member States for e-servicing capabilities, have also been factored in.

95. For ECLAC, the upgrade of its local ICT infrastructure with stronger connectivity and a proper backup data centre, and the upgrade of its auditorium and training facilities, are likely to be the most demanding in resources; a very preliminary estimate that is emerging is about \$42 million over 11 years. E-servicing and digital delivery of programmatic activities, especially of intellectual products, to its constituent Member States are also pressing needs. Upgrades and renovations of its 56-year-old building, especially for resilience as well as sustainability, are also being assessed.

96. Economic and Social Commission for Western Asia. The United Nations House in Beirut, which houses ESCWA, has not been renovated since it was built in 1997. The explosion at the Beirut port in 2020 damaged the buildings and general infrastructure of the ESCWA complex, with repair work, which started in 2020, still under way. Demands for new servicing modalities are putting pressure on ESCWA infrastructure, as in the case of ECLAC. The highest resource needs of ESCWA are likely to be for its local ICT and conferencing infrastructure, totalling about \$14 million over multiple years. The renovations to the buildings are likely to be the second largest need.

97. United Nations Office at Geneva. The initial assessment of the United Nations Office at Geneva covers the Palais des Nations campus in Geneva, with a focus on the buildings, facilities and areas not covered by the ongoing strategic heritage plan project of the Office, which is scheduled for completion in 2025.

98. The campus currently includes 33 buildings and structures across 114 acres (46 hectares) within a perimeter of 3.5 kilometres. The assessment of the United Nations Office at Geneva covers the preservation of its archives and library, as well as the preservation of the investments under the strategic heritage plan after its completion.<sup>3</sup> The upgrade of its local ICT infrastructure is likely to be relatively large and will have to be weighed in the context of the overall ICT strategy and its impact on local ICT infrastructure. Similarly, the use of its buildings, which is not covered by the plan, will have to be reviewed in the context of the new work modalities. The United Nations Office at Geneva is contemplating a comprehensive technical review to determine the plans for its structures based on long-term operational requirements or preservation needs.

99. United Nations Office at Nairobi. The Gigiri complex in Nairobi encompasses 41 building structures across 148 acres of land within a perimeter of 13 kilometres. The United Nations Office at Nairobi assessment included consideration of the two construction projects in progress, scheduled for completion through 2025 and 2030, namely: (a) the upgrade of office blocks A–J, which have reached the end of their life, along with the redesign of office blocks M–X to implement a flexible work environment, which is scheduled for completion by 2025, will increase office space utilization by 25 per cent; and (b) the Nairobi conference centre project currently under consideration, scheduled for substantial completion by 2029. Besides needing its local ICT

<sup>&</sup>lt;sup>3</sup> See General Assembly resolution 75/253, in which the conclusions and recommendations contained in a related report of the Advisory Committee on Administrative and Budgetary Questions (A/75/7/Add.12) are endorsed.

infrastructure, the Office is also likely to need vehicles for fire safety, security patrol and ambulances. The Office has demands for office space in the Gigiri complex from other United Nations entities who may be willing to invest in such assets.

100. Economic Commission for Africa. The ECA campus has grown to become a consolidated One United Nations system complex, encompassing 20 buildings and over 110,000 m<sup>2</sup> of construction within 13 hectares of land surrounded by 1.6 km of perimeter. It hosts around 2,250 personnel of ECA and various agencies of the United Nations system. Around 70 per cent of the 1,897 personnel of the United Nations agencies in Addis Ababa continue to wait for space at the ECA campus to relocate. In addition to its headquarters in Addis Ababa, ECA maintains six offices across the African continent, including five subregional offices and the African Institute for Economic Development and Planning, based in Dakar. Two such offices are located on United Nations-owned premises (Lusaka and Yaoundé), and four are in leased premises (Rabat, Kigali, Dakar and Niamey).

101. The construction of the ECA campus was begun in 1961 with the Congo Building and Africa Hall, continuing in 1974–1976 (the Niger, Limpopo and Nile Buildings) and followed by the construction of the Conference Centre in 1996 and of the Zambezi Building in 2011. No significant recapitalization has been undertaken besides maintenance and ad hoc repairs, except for the ongoing projects of the Africa Hall renovation (1961), the upgrade of two rooms of the Conference Centre (2011) and the pilot flexible workspace project in the Niger Building (1976), all scheduled for completion during 2023–2024. While important, these investments cover only a fraction of the accumulated requirements, as noted in the report of the Secretary-General on the strategic capital review (A/72/393) and by the Advisory Committee in its related report (A/72/7/Add.9).

102. The international standard for the life cycle of building structures is 40 years, with periodic upgrades to maintain value and operational efficiency. Such maintenance and refurbishments at ECA during 1982–2022 have extended the life of these assets by 50 per cent, to 60 years. Notwithstanding this, ECA buildings are among the most depreciated.

103. ECA will need not only local ICT and conferencing infrastructure upgrades but probably even more upgrades to structures as well. The ECA clinic will also need investments,<sup>4</sup> considering its criticality for the United Nations community in Addis Ababa. Given the likely scale of its requirements over time, a comprehensive technical assessment during 2023 is considered essential for ECA. A strong internal project management capacity may also be needed to provide stewardship for these time-sensitive initiatives.

104. In August 2022, the Department of Safety and Security conducted a technical assessment at ECA that highlighted the urgency of some upgrades for compliance with minimum operating security standards, given the elevated risk level at the duty station since November 2021. For 2023, in addition to upgrades of the access control systems and networks across campus, the other priority requirements are:

(a) The overhauling of the main entrance gate to the ECA campus (East Gate 2) to segregate pedestrian and vehicular access for risk mitigation for key long-term security mitigation and enhancement of compliance with minimum operating security standards;

(b) The strengthening of the 1.6-km perimeter of the ECA campus will involve construction-related overhauling of adjacent structures and gates to reinforce protection, such as of the north car park, or installation of a protection screen/roof to mitigate the line-of-sight risk from neighbouring tall buildings;

<sup>&</sup>lt;sup>4</sup> As endorsed by the General Assembly in its resolution 76/245. See A/76/7, para. XI.8.

(c) The initial stage of upgraded ballistic protection and structural hardening across lobbies and pathways campus-wide, currently lacking capabilities regarding minimum operating security standards, starting with the Conference Centre and the Niger and Zambezi Buildings.

105. Starting in 2023, the strengthening of the perimeter and related implementation would be the first, urgent step of the upgrade of physical security protection of the ECA campus. Equally, the requirements to implement ballistic protection and hardening of all entrances, lobbies of the various buildings and pathways across campus will also require extensive cross-integration among construction, engineering, cabling, energy and underlying ICT infrastructure implementation. Another cross-implementation requirement regarding compliance with minimum operating security standards concerns fire safety, specifically the need to enhance engineering capacity for the supply and storage of water across campus.

106. In view of the current lack of compliance with minimum operating security standards, and owing to the heightened security situation in Addis Ababa, ECA will urgently need resources, during 2023, to initiate these projects on the path to compliance with the standards. To avoid suboptimal investments while striving for compliance with the standards, it is also important to fund, during 2023, the technical consultancy to help ECA to produce a detailed plan that will form the basis for a report to be submitted to the General Assembly, ideally during its the seventy-eighth session.

107. Accordingly, the Secretary-General proposes additional resources amounting to \$5,488,000 under section 33 of the proposed programme budget for 2023 to initiate the implementation of minimum operating security standards compliance and related requirements, as detailed in table 11.

# Table 11Resource requirements for 2023

(Thousands of United States dollars)

		2023 estimate (before recosting)
A. Alteration, upgrades and major maintenance programmes		
Technical design consultancy		700.1
Subtotal, alteration, upgrades and major maintenance programmes		700.1
B. Safety and security upgrades		
<ul> <li>A. Alteration, upgrades and major maintenance programmes         Technical design consultancy         Subtotal, alteration, upgrades and major maintenance programmes     </li> <li>B. Safety and security upgrades         Upgrades for minimum operating security standards compliance with associated infrastructure upgrades across campus: perimeter strengthening, ballistic protection and upgrade of safety and security services systems     </li> <li>Upgrades for minimum operating security standards compliance with associated infrastructure across campus: perimeter strengthening, ballistic protection and upgrade of safety and security services systems     </li> <li>Upgrades for minimum operating security standards compliance with associated infrastructure across campus: north car park, shielding of Conference Centre entrance for dignitaries and very important persons, and fire safety     </li> <li>Subtotal, safety and security upgrades</li> </ul>	Security, facilities and accessibility with upgraded protection features (initial stages)	3 588.0
upgrade of safety and security services systems	Safety/security	299.9
Upgrades for minimum operating security standards compliance with associated infrastructure across campus: north car park, shielding of Conference Centre entrance for	Fire safety and business continuity, security (initial stage)	
dignitaries and very important persons, and fire safety		900.0
Subtotal, safety and security upgrades		4 787.9
Total		5 488.0

108. As explained above, assessments in relation to the offices at United Nations Headquarters, the Economic and Social Commission for Asia and the Pacific and the United Nations Office at Vienna will be undertaken later and completed by the first quarter of 2023.

### VI. Action to be taken by the General Assembly

109. The General Assembly is requested:

(a) To take note of the present report;

(b) To approve the establishment of four posts (P-4) and six general temporary assistance positions (three P-2 and three General Service (Principal level)) in 2023;

(c) To appropriate an additional amount of \$5,488,000 under section 33, Construction, alteration, improvement and major maintenance, and an additional amount of \$6,662,700 under section 29C, Office of Information and Communications Technology, both under the proposed programme budget for 2023, which would represent a charge against the contingency fund;

(d) To appropriate an additional amount of \$100,400 under section 36, Staff assessment, of the proposed programme budget for 2023, to be offset by an equivalent increase of \$100,400 under income section 1, Income from staff assessment;

(e) To take note that the Secretary-General intends to submit reports on cybersecurity, physical security and capital investment planning during the General Assembly at its seventy-eighth session.

## Annex I

22-23094

## Cybersecurity current capacity and gaps

### Distribution of headcount by cybersecurity work stream and duty station: current vs. gap/new positions



Cybersecurity work stream by duty station

A/77/519

## Sa Annex II

## Preliminary estimates for safety and security resources for 11 years (2024–2034)

### Table 1

Breakdown of investment requirements for safety and security services by subcategory and duty station with preliminary estimates, 2023–2034 (initial 2022 exercise)

Duty station		2023		2024		2025		2026		2027		2028		2029		2030		2031		2032	2033		2034	Total No.	Tota	Total subprojects
	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate	No.	Estimate No.	Estimate	No.	Estimate	of project series, 2023–2034	estimate, 2023–2034	<i>subprojects</i> , by area, 4 2023–2034
ECA	2	299 880	12	314 475	20	2 354 425	26	4 013 150	12	5 547 790	2	1 085 780	-	-	3	848 000	3	1 060 000	1	212 000 -	-	-	-	30	15 735 500	81
Security systems (various assets)	-	-	6	157 238	6	354 577	9	495 038	3	53 000	-	-	-	-	-	-	-	-	-		-	-	-	9	-	-
Physical security infrastructure	2	299 880	6	157 238	14	1 999 848	17	3 518 113	9	5 494 790	2	1 085 780	-	-	3	848 000	3	1 060 000	1	212 000 -	-	-	-	21	-	-
ECLAC	-	-	6	1 673 196	6	1 754 130	4	1 530 000	5	860 000	4	750 000	3	400 000	2	340 000	2	340 000	2	340 000 2	340 000	2	340 000	10	8 667 326	38
Security systems (various assets)	-	-	4	1 483 196	4	862 130	3	930 000	5	860 000	4	750 000	3	400 000	2	340 000	2	340 000	2	340 000 2	340 000	2	340 000	7	-	-
Physical security infrastructure	-	-	1	160 000	2	892 000	1	600 000	-	-	-	-	-	-	-	-	-	-	-		-	-	-	2	-	-
Technical consultancy	-	-	1	30 000	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		-	-	-	1	-	-
ESCAP	-	-	5	560 000	2	317 000	5	470 000	3	310 000	3	220 000	-	-	-	-	1	330 000	-	- 1	200 000	1	200 000	17	2 607 000	21
Security systems (various assets)	-	-	4	460 000	1	142 000	4	270 000	2	210 000	3	220 000	-	-	-	-	1	330 000	-	- 1	200 000	1	200 000	15	-	-
Physical security infrastructure	-	-	1	100 000	1	175 000	1	200 000	1	100 000	-	-	-	-	-	-	-	-	-		-	-	-	2	-	-
ESCWA (subprojects)	-	-	4	4 200 000	3	1 220 000	3	640 000	3	550 000	1	100 000	2	150 000	2	220 000	5	$1\ 010\ 000$	2	400 000 1	100 000	2	150 000	8	8 740 000	28
Security systems (various assets)	-	-	1	100 000	1	100 000	3	640 000	2	400 000	1	100 000	1	100 000	1	100 000	3	640 000	2	400 000 1	100 000	1	100 000	4	-	-
Physical security infrastructure	-	-	3	4 100 000	2	1 120 000	-	-	1	150 000	-	-	1	50 000	1	120 000	2	370 000	-		-	1	50 000	4	-	-
United Nations Headquarters	-	-	21	5 666 160	11	2 843 159	9	2 443 159	8	998 159	6	498 159	7	893 159	5	453 159	4	253 159	4	253 159 5	283 159	7	1 083 159	22	15 667 750	87
Security systems (various assets)	-	-	11	2 996 160	7	2 143 159	8	2 343 159	7	898 159	6	498 159	7	893 159	5	453 159	4	253 159	4	253 159 5	283 159	7	1 083 159	12	-	-
Physical security infrastructure	-	-	9	40 000	4	-	1	-	1	-	-	-	-	-	-	-	-	-	-		-	-	-	9	-	-
Fire safety/vehicle	-	-	1	2 630 000	-	700 000	-	100 000	-	100 000	-	-	-	-	-	-	-	-	-		-	-	-	1	-	-
United Nations Office at Geneva	-	-	4	2 367 000	5	5 767 000	3	4 400 000	1	500 000	-	-	-	-	-	-	1	500 000	-		-	1	500 000	7	14 034 000	15
Security systems (various assets)	-	-	3	1 867 000	2	3 367 000	1	2 500 000	1	500 000	-	-	-	-	-	-	1	500 000	-		-	1	500 000	4	-	-
Physical security infrastructure	-	-	1	500 000	3	2 400 000	2	1 900 000	-	-	-	-	-	-	-	-	-	-	-		-	-	-	3	-	-
United Nations Office at Nairobi	-	-	45	4 071 885	17	191 500	21	304 500	19	345 500	23	1 593 500	26	698 833	18	201 500	18	209 500	24	1 322 500 22	840 834	22	1 014 000	50	10 794 052	255
Security systems (various assets)	-	-	33	2 433 052	15	156 500	18	259 500	17	310 500	20	1 458 500	21	516 000	16	166 500	16	174 500	22	1 287 500 18	584 500	19	959 000	36	-	-
Physical security infrastructure	-	-	9	156 333	-	35 000	1	35 000	-	35 000	1	35 000	2	156 333	-	35 000	-	35 000	-	35 000 1	156 334	1	35 000	11	-	-
Fire safety/vehicle	-	-	3	1 482 500	2	-	2	10 000	2	-	2	100 000	3	26 500	2	-	2	-	2	- 3	100 000	2	20 000	3	-	-
United Nations Office at Vienna	-	-	5	3 750 000	3	750 000	6	$1\ 080\ 000$	7	2 370 000	9	2 670 000	8	870 000	9	2 490 000	8	490 000	9	690 000 8	490 000	9	2 490 000	19	18 140 000	81
Security systems (various assets)	-	-	3	650 000	3	750 000	5	$1\ 055\ 000$	5	345 000	8	2 645 000	6	445 000	6	445 000	6	445 000	7	645 000 6	445 000	6	445 000	14	-	-
Physical security infrastructure	-	-	1	3 000 000	-	-	1	25 000	2	2 025 000	1	25 000	2	425 000	3	2 045 000	2	45 000	2	45 000 2	45 000	3	2 045 000	4	-	-
Technical consultancy	-	-	1	100 000	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		-	-	-	1	-	-
Total, projects with estimated requirements by safety and security services category across duty stations, 2023–2034	2	299 880	102	22 602 716	67	15 197 214	77	14 880 809	58	11 481 449	48	6 917 439	46	3 011 992	39	4 552 659	42	4 192 659	42	3 217 659 39	2 253 993	44	5 777 159	163	94 385 628	606

# Table 2Count of project series by category across duty stations, 2023–2034

Category	ECA	ECLAC	ESCAP	ESCWA	United Nations Headquarters	United Nations Office at Geneva	United Nations Office at Nairobi	United Nations Office at Vienna	Total
Security systems (various assets)	9	7	15	4	12	4	36	14	101
Physical security infrastructure	21	2	2	4	9	3	11	4	56
Technical consultancy	_	1	_	_	-	_	_	1	2
Fire safety/vehicle	-	_	_	_	1	-	3	-	4
Total, project series by category	30	10	17	8	22	7	50	19	163

Abbreviations: ECA, Economic Commission for Africa; ECLAC, Economic Commission for Latin America and the Caribbean; ESCAP, Economic and Social Commission for Asia and the Pacific; ESCWA, Economic and Social Commission for Western Asia.