United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

INTERNAL AUDIT DIVISION I
OFFICE OF INTERNAL OVERSIGHT SERVICES

Confidential

TO: Ms. Heidi Tagliavini
A: Special Representative of the Secretary-General
United Nations Observer Mission in Georgia (UNOMIG)

DATE: 11 October 2004

REFERENCE: AUD-7-5:15 (0826/04)

FROM: Patricia Azarias, Director
DE: Internal Audit Division I, OIOS

P. Azarias

SUBJECT:
OBJET: **OIOS Audit No. AP2004/656/01: Field Security Procedures in United Nations Observer Mission in Georgia (UNOMIG)**

1. I am pleased to present herewith the final report on the subject audit, which was conducted during the period June-July 2004. The audit was conducted in accordance with the general and specific standards for the professional practice of internal auditing in United Nations organizations and included such tests as the auditors considered necessary.

2. We are pleased to note from your comments on the draft report that important progress has already been made to implement some of the audit recommendations, while others are under active consideration in order to continue to improve overall security procedures. OIOS also notes your point that "Regrettably the audit due to a lack of coordination at the ground level was conducted at the time of the CSOs' workshop in Brindisi, Italy, the Chairperson of the UNOMIG MSMT/DSRSG was on sick leave, and the CAO was on vacation."

3. Based on the comments received our office will perform a follow-up audit of major security procedures. The follow-up is expected to validate actions taken and available supporting evidence. It will also take into account applicable lessons learned and best practices in other peacekeeping missions in consultation with DPKO.

4. Audit recommendations remain open in OIOS' recommendation database pending validation of remedial actions completed. Please refer to the recommendation number concerned to facilitate action planning and monitoring of the implementation status. Also, please note that OIOS considers recommendations 9, 11, 13, 15 and 17, as being of critical importance, and requests that you focus your attention on them.

/...

5. OIOS is assessing the overall quality of its audit process and kindly requests that you consult with your managers who dealt directly with the auditors and complete the attached client satisfaction survey form.

6. I would like to take this opportunity to thank you and your staff for the assistance and cooperation provided to the auditors in connection with this assignment.

Copy to: Mr. Jean-Marie Guehenno, Under-Secretary-General for Peacekeeping Operations
Ms. Diana Russler, Director and Deputy UN Security Coordinator
Ms. Hazel Scott, ASD/DPKO
UN Board of Auditors
Programme Officer, OIOS
Mr. Nikolai Grigoriev, Auditor-in-Charge, IAD I, OIOS
Mr. Gerald Kopil, Resident Auditor, UNMIK, OIOS

Office of Internal Oversight Services

Internal Audit Division I

Audit of Field Security Procedures in UNOMIG

Audit no:	AP2004/656/01
Report date:	11 October 2004
Audit team:	Nikolai Grigoriev, Auditor-in-Charge Gerald Kopil, Auditor

EXECUTIVE SUMMARY
Audit of Field Security Procedures in UNOMIG – AP2004/656/01

In view of the changing security environment and threats worldwide, the Office of Internal Oversight Services (OIOS), Department of Peacekeeping Operations (DPKO) and the Office of the United Nations Security Coordinator (UNSECOORD) identified the audit of global field security procedures as a matter of priority.

The Security Council, General Assembly and Secretary-General have issued several policy documents, including the lessons learned report on Iraq dated 4 March 2004, recognizing the paramount importance of security and safety of UN personnel in the field. In one of these documents [A/57/365 of 28 August 2002], the Secretary-General set out an inter-organizational security framework for accountability for the United Nations field security management system. The document states unambiguously the responsibilities of every entity, individual and group of individuals within the United Nations system of organizations involved in the management of security. DPKO has initiated reforms to its security operations in peacekeeping missions with the issuance of the new DPKO Policy and Standard Operating Procedures (SOPs) for a trial period of one year effective October 2003.

This report assesses the capability and readiness of UNOMIG Security Section in carrying out effectively its mandate for staff safety and security in the Mission area. It also assesses the Mission's performance against the established accountability framework and SOPs. The report discusses policy and procedural issues that are associated with the security of UN personnel and assets and provides practical recommendations for improving security management.

Based on the audit work performed, we noted the need for improvements in the planning, coordination, and control of the Security function in the Mission to ensure the capability and readiness of the Security Section in performing its mandate and the operational application of the accountability framework. Of concern were the following issues:

- The Chief Security Officer (CSO) did not report directly to the SRSG but to the Chief Administrative Officer (CAO). There is a need to change the reporting relation to enhance the importance and transparency of the security function.

- A documented management framework linking CSO, Chief Military Officer (CMO) and Civilian Police for the implementation of security policy in the case of a crisis did not exist. There is a need for the respective security responsibilities and accountabilities of the Chief Security Officer and the Designated Officials in the area of Security management and field operations to be communicated to all staff concerned.

- UNOMIG did not develop and maintain a computerized information database of "Security" lessons learned.

- There is a need for the Mission to prepare a crisis management plan, which includes an analysis of risk scenarios, or options for potential contingencies.

- There is need for a drill plan to be prepared and executed at all major locations at Headquarters and the Regions. The plan should provide for various types of drills including fire, medical and crisis evacuation.

- The Mission did not have a security information and coordination function comprising qualified staff at the appropriate levels. There is need to communicate the relative management and operational roles at UNOMIG for information sharing and methods of operations to Civilian Police and military officials in charge of security aspects in the Mission.

- The Mission did not conduct a compliance inspection to ensure minimum MOSS requirements for AOR are complied with and its recommendations implemented. An appropriate management action plan to address findings of the MOSS review should be prepared, and the extent of implementation of corrective measures followed up.

- The Mission did not prepare annual work plans for the Security Section, which should taken into account key risk security areas based by a systematic threat assessment of operations in Tbilisi, Headquarters and the regions. The work plans should specifically indicate risks and or initiatives together with the objectives, activities, and the necessary resources to implement them including realistic estimated milestones.

- There is need to carry out a cost benefit analysis prior to renewal of the AITAR rental lease for UNOMIG on 1 January, 2005, to determine the costs and benefits of Headquarters remaining at the present location in Sukhumi, strengthening access controls or relocating to a new site.

- There is also a need for the Mission to assess whether existing risks of unauthorized access in both Zugdidi and Sukhumi may be reduced through the purchase and use of an X-Ray machine. Blast proof protective film should be installed on the windows of the office buildings in Zugdidi.

In our opinion, the correction of the deficiencies identified in this report will promote a culture of awareness and a sustained commitment to the UN security management programme. Management should develop an action plan to address observations and recommended improvements contained in this report.

TABLE OF CONTENTS

I. INTRODUCTION

1. The results of the audit of the OIOS-IAD I on the security function of UNOMIG are discussed in this report. The audit was carried out in accordance with the standards for the professional practice of internal auditing in United Nations Organizations.

2. The Mandate of the United Nations Observer Mission in Georgia (UNOMIG) was originally established by Security Council resolution 858 (August 1993). The Mission mandate was expanded and extended a number of times. Resolution 1524 (January 2004) extends its mandate until 31 July 2004. This mission is further divided into four areas namely Tbilisi, Sukhumi, Gali and Zugdidi. Mission Headquarters is located in Sukhumi.

3. In UNOMIG, the Special Representative of the Secretary General (SRSG) for Georgia has been appointed as the Designated Official (DO) for security in Abkhazia including areas of Restricted Weapons Zone. The UNDP Resident Representative is the DO for security in Georgia including Tbilisi. The DO is accountable to the UN Secretary General, through the UN Security Coordinator (UNSECOORD), for the security and safety of all UN personnel and property in the Mission area. The Special Representative of the Secretary-General in Tbilisi is assisted by a Deputy Special Representative of the Secretary-General in Sukhumi, both responsible for overall mission direction and management.

4. The approved budget of UNOMIG for the year 1 July 2003 - 30 June 2004 is $32.1 million. Strength as at 30 June 2004 includes 121 military observers and 11 civilian police supported by 100 international civilian personnel and 182 local civilian staff. Security is the largest section in the UNOMIG mission with 47 authorized posts for international security officers and 28 authorized posts for local staff. In addition, UNOMIG has outsourced 63 security staff from the Higher Abkhaz Authority, as internal and external guards in Sukhumi and Tbilisi, at a cost of $108,000 per annum.

II. AUDIT OBJECTIVES

5. The overall objective of the audit was to assess the capability and readiness of UNOMIG Security Section in carrying out effectively its mandate for staff safety and security in the Mission area. It also was to review the Mission's performance against the established accountability framework and Standard Operating Procedures (SOPs). Specific objectives are to review and assess whether: (i) the Mission has adequate security policy and guidance; (ii) adequate security plan and procedures that address evacuation, medevac and major emergencies has been implemented; (iii) in country and in mission coordination is timely and effective; (iv) staff are sufficiently informed on security matters; (v) the level of security education and training is adequate; and (vi) the present levels of staffing and available equipment meet minimum security needs of the Mission.

III. AUDIT SCOPE AND METHODOLOGY

6. The audit included interviews with UNOMIG staff and a review of documents made available to the auditors at the time of the audit. Key personnel such as the CSO, Chairperson of the UNOMIG MSMT/DSRSG and the CAO were not available during the audit due to prior commitments and leave. Detailed discussions were however held with the OIC Security/DCSO and other UNOMIG personnel including the SRSG. Audit coverage included a sample of security operations in Tbilisi, Sukhumi and Zugdidi.

IV. OVERALL ASSESSMENT

7. The field security procedures of UNOMIG should be strengthened. Security of the premises in Sukhumi needs improvement. In that regard, a thorough review and evaluation of the AITAR lease, reporting relationships and the recruitment and training of the security staff would be beneficial. UNOMIG should develop and maintain a centralized and computerized information database of "Security" lessons learned based in part on issues discussed at MSMT meetings. Internet links could also be established with DPKO and a number of relevant Peacekeeping missions worldwide. To facilitate future planning, training and decision-making, security related lessons learned and a database should be developed by UNOMIG in consultation with DPKO and UNSECOORD to capture such lessons.

8. There is need to develop a more comprehensive security plan which should include the crisis management plan and a drill plan that will actually test the warden system. Performance measures and indicators in budget documents should be included and work plans for the Security section need to be prepared for high-risk areas. The SOPs currently being revised by the CSO should be completed and a security information and coordination function should be established.

V. AUDIT FINDINGS AND RECOMMENDATIONS

A. Performance Indicators and Baseline Data

Budget and Performance Indicators

9. The Mission receives total budget estimates from the OPPBA. However, the breakdown of these budget estimates does not specifically identify expenditures related to security at the Mission level. Furthermore, assumptions, performance measures and expected accomplishments were not clearly set out in accordance with Results Based Budgeting (RBB) format in the budget documents. In addition, the security equipment needs of the Mission were not easily identifiable in the financial documents.

Recommendations 1 – 2

The SRSG should ensure that:

(i) UNOMIG, in coordination with OPPBA, should take steps to ensure that the security budget of the Mission is used as a planning tool. Performance indicators should reflect the global issues of strategy and coordination, including the establishment and testing of operational plans (AP2004/656/01/01); and

(ii) The Budget and supporting financial documents are completely and clearly defined in order to adequately measure performance and progress and expected accomplishments for Mission Security. There should be a separate budget line for security (AP2004/656/01/02).

10. *UNOMIG welcomes the auditor's recommendations for enhancing the role of security budgets as a planning tool and the visibility of security expenditures through a dedicated budget line. However, as the budgets of DPKO missions are prepared according to formats defined in and*

by the Headquarters, both of those issues will have to be addressed at that level. OIOS agrees and will keep this recommendation open in its database pending implementation.

Reporting Lines and Performance Evaluation

11. The audit noted that the Chief Security Officer did not report to the Head of Mission or the D/SRSG, as the designated official on security matters, which is not in conformity with the DPKO Field Security Policy. One of several organizational charts that were provided to the auditors showed that the Chief Security Section was reporting to the Chief Administrative Officer rather than to the Deputy SRSG. The DOA also evaluates the CSO's performance and prepares his E-PAS. If needed, however, the CSO can have direct access to the Head of Mission or the D/SRSG.

Recommendation 3

The SRSG should ensure that, in order to stress the importance and transparency of security in the Mission, the CSO should report directly to the D/SRSG and not to the CAO (AP2004/656/01/03).

12. *The CSO stated that UNOMIG reports to the Chairperson MSMT /DSRSG and HOM/SRSG in accordance with the policy guidelines in DPKO Security SOP. The said organizational chart has been misinterpreted. It indicated the location of Security Section, which is under the Office of CAO, not the reporting lines of CSO and was titled as "Organizational Chart of Office of CAO". The misinterpretation was clarified by the OIC Security and he explained that CSO has unrestricted access to the SRSG and DSRSG on all security matters. For clarity we refer to the appointment letter of CMO as a member of MSMT.*

13. OIOS notes the CSO's comments, however feels that organization charts should typically indicate reporting relationships and not only "location". The fact that the internal field mission vacancy notice states that the CSO is under the direct supervision of the CAO, and performance appraisals of the CSO were prepared by the CAO is a further indicator of reporting lines. OIOS will keep this recommendation open in its database pending implementation.

B. Policy, Direction and Guidance

Security Policy, Direction and Guidance

14. There is no evidence that the Mission has issued a security policy that describes specific UNOMIG responsibilities, authorities and accountabilities, and the implementation of DPKO field security. An example would be a security policy statement by the SRSG communicating the overall intent, objectives, significant roles and responsibilities and authorities regarding key personnel charged with implementation aspects UNOMIG Security Policy.

Recommendation 4

The SRSG/DO should ensure that a policy statement on security is systematically communicated to staff on a need to know basis (AP2004/656/01/04).

15. *The Mission indicated that it has issued an authoritative Security Policy underlining specific responsibility, authorities and accountability in the UNOMIG Security Plan (Chapter IV and VI). This was promulgated by SRSG/HOM on 21 October 2003.* OIOS will follow-up to validate implementation action taken.

16. The Mission did not establish procedures for the identification of the security-related lessons learned and best practices as a result of actual security incidents. Furthermore, a centralized database of lessons learned and best practices for UNOMIG and other related peacekeeping missions do not exist. As a result, valuable lessons learned may be lost or not readily available for planning and implementation of good field management practices, field security policies and staff training procedures.

Recommendation 5

The SRSG/DO should ensure that UNOMIG develop and maintain a centralized and computerized information database of "Security" lessons learned. Internet links should also be established with DPKO and a number of relevant Peacekeeping missions worldwide, which would provide UNOMIG with a sound basis for developing better classroom and on-the-job training programmes for Security Officers (AP2004/656/01/05).

17. *The Mission feels that it is already sharing lessons learned with DPKO and UNSECOORD on a routine basis, and that developing a database was never a requirement set by UNSECOORD or DPKO.* The audit team recommends a centralized and computerized information database of "Security" lessons learned based in part on issues discussed at MSMT meetings. Internet links could also be established with DPKO and a number of relevant Peacekeeping missions worldwide. To facilitate future planning, training and decision-making, security related lessons learned and a database should be developed by UNOMIG in consultation with DPKO and UNSECOORD to capture such lessons. OIOS will keep this recommendation open in its database pending implementation.

<u>Security Responsibilities, Accountability Framework and Working Relationships</u>

18. There is no evidence of a documented management framework which links the structure, coordination of roles, information sharing and actual methods of operations among the CSO, CMO and Civilian Police for the implementation of security policy in the case of a crisis. Such a framework is needed to ensure adequate and timely management response in the case of an emergency.

19. Based on limited interviews with available staff, there does not appear to be a full awareness of the respective security responsibilities, accountabilities and working relationships with regards to the roles and linkage played by the Designated Officials for the country and individual sectors/regions.

Recommendation 6

The SRSG should request UNSECOORD and DPKO to formalize a management framework linking and outlining roles and responsibilities of the Chief Security Officer, CMO and Civilian

Police for the implementation of security policy in the case of a crisis, and communicate the respective security responsibilities and accountabilities of the Chief Security Officer and the Designated Officials to all staff concerned (AP2004/656/01/06).

20. *The Mission stated that the UNOMIG Security Plan not only clearly outlines the security management structure for all components of the Mission but also delineates the specific responsibilities and accountability of all concerned such as CMO and Senior CIVPOL Advisor at Paragraphs 3, 4, 5 and 6 of Section VI. In addition, roles and working relationship of the different members of the MSMT were further clarified in the formal appointment letters. As a specimen, they attached an appointment letter of the current CMO as a member of MSMT. Accordingly they feel there is no perceived utility in soliciting further formal guidelines from UNSECOORD and DPKO.*

21. OIOS welcomes the fact that the Mission provides the example of the appointment letter of the current CMO as a member of MSMT to clarify the responsibility and accountability framework. However, it covers only a single issue, when a Military Sector Commander is appointed as a Sector Security Coordinator. Further, the phrase that he is expected to coordinate all his security related actions with the CSO is rather vague. A deeper and more global approach is needed. That is why the audit mentions the framework linking the structure, coordination of roles, information sharing and actual operating methods. The interview with one of the Military Sector Commanders also showed the necessity to reinforce the link between military and security components of the Mission. OIOS will keep this recommendation open in its database pending implementation.

C. Security Plans

Crisis Management Plan

22. According to Section XVI of the UNOMIG Security Plan, Mission the Security Management Team (MSMT) had to develop a crisis management plan, including possible scenarios, such as kidnapping, death, arrest or detention of a staff member, or various natural disasters. However, we were not provided with evidence of the existence of a crisis management plan.

Recommendation 7

The SRSG/DO should develop a crisis management plan that takes into account previous lessons learned which includes an analysis of scenarios or options for potential contingencies (AP2004/656/01/07).

23. *The Mission feels that the Crisis Management Plan, as available at Chapter XVI of UNOMIG Security Plan, is essentially describing the process of dealing with any contingencies by the MSMT and Crisis Management Group (CMG). They do not perceive any natural disaster in the Mission area and as such this contingency did not form part of our Security Plan.*

24. *UNOMIG makes further reference to Field Security Handbook, 1 January 1995, Annex B, "Guidelines for Preparation of a County Specific Security Plan". The said document indicates, "The Security Plan will contain information regarding the following: Summary of Security Situation at Duty Station, Officials Responsible for Security, Listing of Internationally-Recruited Staff and Dependants, Listing of Locally-Recruited Staff and Dependants. Division of Country/City into*

Zones and Communication". Hence, clearly UNOMIG Security Plan is all inclusive and the Warden Drill Plan is not a recommended element of a Security Plan.

25. Although the Mission states that it has sufficient guidelines for dealing with all emergencies and contingencies in the Security Plan, the OIOS audit team believes that a more "down to earth" planning and military type SOPs (envelopes with concrete scenarios) are necessary in cases in emergency situations and in cases of kidnapping, death arrest detention etc. Events in other missions demonstrated the need for such an approach, since the Security Plan did not withstand the reality test. OIOS will keep this recommendation open in its database pending implementation.

Warden System

26. Drills or rehearsals to simulate emergency situations have not been carried out in all UNOMIG locations. A plan for complete coverage of drills at UNOMIG locations has also not been prepared. As a result, the level of the Mission's preparedness to confront these emergency situations in a timely and professional manner might be compromised.

Recommendation 8

The SRSG should ensure that a drill plan is prepared and executed at all major locations at Headquarters and the Regions. The plan should provide for various types of drills including fire, medical and crisis evacuation (AP2004/656/01/08).

27. *The Mission feels that appropriate exercises have been prepared and conducted. It states that "UNOMIG has successfully conducted evacuation exercises and training, where not only the warden drills but also all other provisions relevant to contingencies/crisis have been rehearsed/tested".* OIOS notes the comments of UNOMIG, however, no documental evidence of the actions taken had been provided to the auditor at the time of the audit. OIOS will keep this recommendation open in its database pending receipt of supporting documents.

D. Security Management Standing Operating Procedures

28. The audit noted that Standard Operating Procedures (SOPs) for emergency situations were not developed. In addition, Mission Standard Operating Procedures for UNOMIG have not yet been drafted or finalized by the CSO. The last SOPs were prepared by the CMO in 2001.

Recommendation 9

The SRSG/DSRSG should complete and sign off on the Standard Operating Procedures and distribute it to all staff concerned (AP2004/656/01/9).

29. *The Mission states that UNOMIG has sufficient guidelines for dealing with all emergencies and contingencies in the Security Plan. In addition, all personnel have been briefed and participated in exercises and associated training and regular security advisories were promulgated to all Mission personnel.* OIOS will keep this recommendation open in its database pending implementation.

E. Coordination among Offices and Other Bodies

30. The Security Office did not have a security information and coordination function which deals with issues of liaison, monitoring and forecasting. The Administrative Assistant performed these duties. Coordination between different parts of the Mission needed improvement. Chief of CIVPOL and CMO were not well aware of the details of the Mission Security Plan.

31. There exists a risk that this lack of coordination may lead to confusion and delayed actions in the event of a crisis. In that regard, information sharing especially with regards to plans, drills and lessons learned in actual field operations would be useful.

Recommendation 10

> The SRSG/D/SRSG should establish a security information and coordination function, which comprise qualified staff at the appropriate levels. The relative management and operational roles of key players at UNOMIG for information sharing and methods of operations should also be communicated to Civilian Police and military officials in charge of security aspects in the Mission (AP2004/656/01/10).

32. *The Mission stated that the establishment of a separate Security Information and Coordination Cell is not considered appropriate since each DPKO Mission is unique of its own nature and one should not be compared with another. UNMIK has a much greater number of Security officers apart from a huge military. UNMIK has a much greater number of Security officers apart from a huge military, CIVPOL contingents and KFOR sharing most of the security needs of the Mission. A mission like UNMIK can afford to have a separate Security Information and Coordination Center/cell. Unfortunately, this is not possible for UNOMIG with a much smaller Security section. However, in our 05/06 budget submission provision of two additional professional level security officers has been requested and this may permit the establishment of such information and coordination cell in the future. It should be noted that CSO is the only professional level Security officer in UNOMIG Security at present.*

33. *CSO/DCSO and all Security Team Leaders however are performing the functions of security information and coordination on a daily basis. As a result, MSMT is fully apprised of key security related issues and all mission personnel are kept posted/advised through regularly issued "security advisories". Both the Senior CIVPOL Advisor and CMO were also personally briefed by CSO on all security matters including the Security Plan immediately upon their arrivals and have been provided with individual copies of the Mission Security Plan.*

34. OIOS feels that UNOMIG should evaluate the feasibility of having a Security and Coordination Cell taking into account all costs and benefits including mitigating safety and security risks of UNOMIG staff that must operate in so many different locations. OIOS will follow-up on the results of the UNOMIG evaluation and keep this recommendation open in its database pending implementation.

F. Security Education, Training and Activities

MOSS Review

35. The auditors were not provided with a document outlining steps to be taken after the MOSS review was performed in 2003. There was also no evidence that corrective measures were actively followed up.

Recommendation 11

The SRSG/D/SRSG should prepare an appropriate management action plan which addresses the findings of the MOSS review and the extent of implementation of corrective measures (AP2004/656/01/11)

36. *The Mission stated that MOSS was never approved by DPKO as a policy for implementation. During the last CSOs' Workshop in Turin in June 2003 the foundation of MOSS was laid which was further developed during the Brindisi CSOs' Workshop in July 2004. However, on its own initiative, UNOMIG has taken steps and has submitted budgetary requirements to attain the baseline MOSS as was drafted in June 2003. Currently UNOMIG is MOSS compliant with the baseline requirement agreed during CSOs' Workshop in Brindisi in July 2004.*

37. OIOS commends UNOMIG on its initiatives and will keep this recommendation open in its database pending implementation.

Training of Security Officers

38. Except for the qualified firearms training, the security officers of UNOMIG did not receive sufficient training.

Recommendation 12

The SRSG/DO should develop a comprehensive training programme, including management practices for the sector team leaders, as well as other types of training such as first aid (AP2004/656/01/12).

39. *The Mission stated that formal training courses for Security officers are unfortunately extremely limited throughout the UN system. Deficiencies along the line were discussed during the last CSOs' Workshop in Brindisi and quite a few positive steps have been taken to improve the matter of training in DPKO. In the mean while, training is limited to "on job training" as opposed to more formalized training curriculum due to lack of qualified and well trained Security Officers.*

40. OIOS agrees and feels that a training plan should be prepared to plan and account for both the formal and on job training needs of UNOMIG security personnel. The audit believes that firearms and on the job training is not enough in case of UNOMIG, especially taking into account the need to improve the quality of the Security Officers. OIOS will keep this recommendation open in its database pending implementation.

G. Staffing, Competencies and Planning of Security Office

Work Plans

41. Work plans detailing activities, resources, milestones have not been prepared by the CSO for the management and operations of the Office. Typical key security functions would entail investigations, information gathering, protection, equipment, liaison and training. Criteria for posting staff and manning around the Mission were not available for review.

Recommendation 13

The CSO should prepare work plans for key risk security areas based by a systematic and periodic threat assessment of operations in Tbilisi, Headquarters and the regions. The work plans should specifically indicate risks and or initiatives together with the necessary resources to implement them, including realistic estimated milestones (AP2004/656/01/13).

42. *UNOMIG stated that a detailed Threat Assessment for UNOMIG is available at Annex B of the Security Plan and UNOMIG has taken appropriate measures to mitigate all threats, risks and vulnerabilities. However, threat assessment is a continual process and is reviewed by CSO/MSMT on a regular basis. As a result of our Threat Assessments we have identified the issues/tasks and developed appropriate plans for their implementation. Accordingly the following tasks/requirements were implemented during the last one year apart from complying with all security requirements placed by UNSECOORD and DPKO:*

a. *UNOMIG Threat Assessment was conducted.*
b. *UNOMIG Security Plan was evolved.*
c. *Special attention was given to the personal security of SRSG, her Office and Accommodation.*
d. *Information sharing was stepped up and Security Advisories were issued to all Mission Personnel.*
e. *Budget submissions were made in line of the draft MOSS and DPKO Security SOP.*
f. *Compound Security and access control at all UNOMIG locations were improved.*
g. *Building Evacuation Plans were made for all UNOMIG Offices including SRSG's Office in Tbilisi and were rehearsed on a regular basis.*
h. *Fire Safety Procedures and Exercises were conducted at all UNOMIG locations.*
i. *MSMT Meetings were held on a routine basis where security information was shared and provisions/procedures were reviewed. All minutes of the meetings were shared with UNSECOORD and DPKO Security Focal Point.*
j. *UNOMIG Internal Security Clearance Procedure was developed.*
k. *Evacuation Plan for SRSG's Office in Tbilisi was prepared.*
l. *All Mission personnel in SRSG's Office were briefed on Evacuation Procedures.*
m. *Evacuation Exercises throughout the Mission area were conducted.*
n. *All Mission personnel completed Basic Security in the Field interactive CD ROM.*
o. *Improvement of current Security staffing and organization.*

43. *A rotation plan has been developed by the CSO which entails reassignment of Security Officers within the Mission on a nominal 6 months basis. However, the exigencies of service may delay the 6 months policy guide. As previously indicated, there had been no Security policies available within UNOMIG prior to the arrival of the current CSO. Previously CMO was addressing most of the security issues, which were taken over by the CSO according to DPKO policies.*

44. OIOS notes the improvements made by UNOMIG during the last year as a result of threat assessments, that appropriate plans have been developed, and that issues/tasks have been identified for their implementation. OIOS will follow-up available documentation to validate implementation actions taken.

ID Control System

45. The ID control system based on access cards with photo, signature and expiry dates appear to be working effectively for UN staff. However, access to the compound by unknown Tourgostinitsa AITAR Hotel (AITAR) visitors or guests poses significant risks to UN staff and facilities.

46. Although the existing contract with AITAR appears sound, enforcement (Refer Article 12 Access to Third Parties) regarding the visitors needs to be improved. A cost benefit analysis which includes an assessment of the political realities, investments made to date, and known and potential security concerns and risks may result in such improvements.

Recommendation 14

The SRSG should ensure that, prior to renewal of the AITAR contract on 1 January 2005, a cost benefit analysis is carried out to evaluate the costs and benefits of Headquarters remaining at the present location in Sukhumi, strengthening access controls or relocating to a new site (AP2004/656/01/14).

47. *It is the assessment of this Mission that the current HQ location in the Aitar Hotel, Sukhumi is the most appropriate facility available that affords the best security posture for UNOMIG and its personnel. Furthermore, it should be noted that during the last visit of UNSECOORD Desk Officer and DPKO Security Focal Point, the suitability of this location, with its inherent deficiencies, was nevertheless adjudged to be satisfactory.*

48. The statement is correct. In its comment the Mission refers to the suitability of the location itself, noting its inherent deficiencies. The audit noted that one of the deficiencies was the weak access control to the area by the so-called "guests" of the Aitar Administration and local cars. The staff of the Mission mentioned on several occasions that the entry regime should be strengthened in order to better protect UN staff and property. OIOS will keep this recommendation open in its database pending implementation.

H. Premises and Equipment

Security Equipment

49. Actual equipment on hand has not been inventoried and reconciled to security needs and equipment authorizations to identify any resulting shortage or surplus.

Recommendation 15

The SRSG/DO should ensure that the CSO prepare a list of all security equipment for the security function to demonstrate that available equipment allows a proper discharge of security responsibilities in the Mission (AP2004/656/01/15).

50. *The Mission indicated that unique security equipment and materials have been identified and submitted to the appropriate asset holders for issuance and proper actions and where appropriate has also been incorporated in the budgetary submission.* OIOS is pleased to note the action taken by UNOMIG. OIOS will keep this recommendation open in its database pending validation of implementation action taken.

Facilities for the Security of the Premises

51. In Zugdidi, no blast proof protective film was installed on the windows of the office buildings, including the room where the military observers hold their meetings. Also, no X-Ray machine was installed for security purposes.

52. Although the Mission is constantly utilizing the Sukhumi Airport, no X-Ray machine was installed there either for security purposes. The Mission also does not have equipment to detect letter bombs.

Recommendation 16

The SRSG/DO should assess whether existing risks of unauthorized access in both Zugdidi and Sukhumi may be reduced through the purchase and use of an X-Ray machine. Blast proof protective film should be installed on the windows of the office buildings in Zugdidi (AP2004/656/01/16).

53. *UNOMIG stated that:*

a. Security requirements for blast protection film were identified and recent indications from OMS/DPKO are that the UNOMIG demand has been assigned "Top" priority and that the shipment details will be expedited.

b. X Ray Machines for the UNOMIG compounds have been included in their 2005/06 budget submission.

c. X Ray Machine at Sukhumi Airport is an issue under the purview of the Mission Aviation Safety Officer not CSO. It is now in operation.

d. Letter bomb detectors were included through our 2005/06 budget submission.

54. OIOS welcomes the actions planned and/or taken and will keep this recommendation open in its database pending implementation.

55. A report was prepared specifying the necessary security improvements at the Dacha housing the offices of the SRSG and her immediate staff while working in Sukhumi. We did not get assurances that these improvements have already been implemented.

Recommendation 17

The SRSG should prepare, execute and follow-up an action plan for improvements in security improvements at the Dacha in Sukhumi (AP2004/656/01/17).

56. *UNOMIG indicated that recommendations for the Dacha are under active consideration of the Mission management and preliminary work has commenced.* OIOS will keep this recommendation open in its database pending implementation.

VI. ACKNOWLEDGEMENT

57. We wish to express our appreciation for the assistance and cooperation extended to the auditors by the UNOMIG management and staff.

P. Azarias

Patricia Azarias, Director
Internal Audit Division I, OIOS

ACRONYMS

CAT	Crisis Action Team
CIVPOL	Civilian Police
CMG	Crisis Management Group
CMO	Military Officer
CSO	Chief Security Officer
DO	Designated Official
DOA	Director of Administration
DPKO	Department of Peacekeeping Operations
DSRSG	Deputy Special Representative of the Secretary-General
FSH	Field Security Handbook
MOSS	Minimum Operating Security Standards
MORSS	Minimum Operating Residential Security Standards
MWSP	Mission Wide Security Plan
OPPBA	Office of Programme Planning, Budget and Accounts
RSP	Regional Security Plan
SG	UN Secretary-General
SMT	Security Management Team
MSMT	Mission Security Management Team
SOP	Standing (or Standard) Operating Procedures
SRSG	Special Representative of the Secretary-General
TAC	Threat Assessment Committee
UNHQ NY	United Nations Headquarters, New York
UNOMIG	United Nations Observer Mission in Georgia
UNSECOORD	United Nations Security Coordinator
USG	Under-Secretary-General

United Nations Nations Unies

OIOS/IAD Client Satisfaction Survey

The Internal Audit Division is assessing the overall quality of its audit process. A key element of this assessment involves determining how our clients rate the quality and value added by the audits. As such, I am requesting that you consult with your managers who dealt directly with the auditors, and complete the survey below. I assure you that the information you provide will remain strictly confidential.

Audit Title & Assignment No.: OIOS Audit No. AP2004/656/01: Field Security Procedures in United Nations Observer Mission in Georgia (UNOMIG)

By checking the appropriate circle please rate:

		1 (poor)	2	3	4(excellent)
1.	The extent to which the audit addressed your concerns as a programme manager.	○	○	○	○
2.	The audit staff's understanding of your operations and objectives.	○	○	○	○
3.	The professionalism of the audit staff (communications, integrity, professional knowledge and responsiveness)	○	○	○	○
4.	The quality of the audit report in terms of:				
	-- accuracy and validity of findings and conclusions	○	○	○	○
	-- clarity and conciseness	○	○	○	○
	-- balance and objectivity	○	○	○	○
	-- timeliness	○	○	○	○
5.	The extent to which the audit recommendations were appropriate and helpful.	○	○	○	○
6.	The extent to which your comments were considered by the auditors	○	○	○	○
7.	Your overall satisfaction with the conduct of the audit and its results.	○	○	○	○

Please comment on any areas in which you have rated the audit team's performance as below your expectations. Also, please feel free to provide any further comments you may have on the audit process to let us know what we are doing well and what can be improved.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Name:_____ **Date:**_____

Title:_____

Organization:_____

Thank you for taking the time to fill out this survey. Please send the completed survey form as soon as possible in the enclosed envelope addressed to: Ms. Patricia Azarias, Director, Internal Audit Division - I, OIOS, Room DC2-518 United Nations Headquarters New York, NY 10017 U.S.A. or by fax to: 212-963-8100.