

Confidential

TO: Mr. Gurpur Kumar, Deputy Director,
A: Internal Audit Division,
Office of Internal Oversight Services

DATE: 29 September 2011

REFERENCE:

THROUGH:

S/C DE:

FROM: Anthony Banbury, Assistant Secretary-General
DE: for Field Support

SUBJECT: **Draft OIOS report on the audit of ICT governance and security**
OBJET: **management in peacekeeping missions – Assignment no. AP2011/615/01**

1. I refer to your memorandum dated 25 August 2011, regarding the above-mentioned audit. Please find below DFS comments on the findings and recommendations contained in the draft report.

Audit results and overall assessment

2. DFS is concerned that the overall rating in the report suggests that the risk management, control and governance processes examined were “partially satisfactory”. DFS takes note that the audits of four out of the six peacekeeping missions on which the rating was based, i.e. MONUC, UNMIS, UNMIL and MINUSTAH were conducted as far back as 2008 and 2009. Between 2008 and 2011, DFS/ICTD provided strategic and budgetary guidance to field missions through the annual ICT Roadmap and has made progress, within its limited staff resources, in developing a departmental ICT security framework and supporting implementation of high level policies. OIOS’ assessment which derives primarily from the findings and recommendations in the 2008 and 2009 audits does not reflect an accurate picture of the current situation. For example, it will be noted that out of the 16 recommendations issued by OIOS in its 2010 ICT audit of UNIFIL, 10 or 63 percent were closed in the final report as implemented.

3. ICT governance and security management in the operational environments of peacekeeping missions is an ongoing process and requires a phased approach in its implementation. DFS/ICTD has, over the years, been performing the ICT related aspects of risk management and control with limited resources. Furthermore, risk assessment, risk management, monitoring and reporting requirements spans across business units and the findings identified in these audits should be measured against Organizational standards.

4. Based on our explanation above, DFS is of the view that the overall assessment of partially satisfactory should be reviewed and amended in the final report.

Regulatory framework (paragraphs 45 and 46)

5. The report has acknowledged in paragraph 45 that the ICT security and compliance function in peacekeeping missions are understaffed. The report also notes in the same paragraph that DFS had requested dedicated ICT resources which were not approved by the General Assembly. In this regard, DFS wishes to reiterate that neither ICTD nor peacekeeping missions have the dedicated capacity or resources to conduct the full spectrum of ICT risks and vulnerability assessments, oversight and compliance.

6. Paragraph 46 of the report notes that OICT would complete a comprehensive information security framework by June 2011. A formal risk assessment and management review of ICT risks for developing mitigating actions has to be established at the Organizational level. In the absence of an organization-wide framework, ICTD continues to make its best efforts to undertake a phased implementation of the ICT security framework across peacekeeping missions. Therefore, DFS requests that recommendations 38 and 47 should be redirected to OICT.

Recommendations

7. Please refer to our comments on the recommendations in the attached matrix.

8. Thank you for the opportunity to comment on the draft report. We stand ready to provide any further information that may be required.

cc: Mr. Soon-hong
Mr. Kumar
Ms. Wong

ANNEX I
SUMMARY OF IMPORTANT RECOMMENDATIONS

Assignment No. AT2011/615/01 - Audit of ICT governance and security management in peacekeeping missions

| Para. no. | Recommendation | Accepted? (Yes/No) | Critical/important | Responsible individual | Implementation date | Client comments |
|-----------|---|--------------------|--------------------|------------------------|---------------------|---|
| 18 | DFS/ICTD should develop mechanisms to: (i) facilitate the preparation of ICT strategic plans in the missions to ensure alignment of ICT investments with the strategies of the Organization; (ii) monitor the alignment of the missions' work plans with the Organization's ICT strategy; and (iii) support the establishment of the ICT risk management framework. | No | Important (Medium) | N/A | N/A | <p>i) DFS wishes to clarify that it has consistently aligned its ICT work programme and investments with the strategies of the Organization. DFS provides strategic guidance to field missions on an annual basis in the form of ICT Roadmap (See the attached copy of the 2011/2012 guidance) which reinforces this alignment. Key strategic initiatives including systems standardization and centralization, infrastructure consolidation and increased use of green technologies and harmonization of ICT organizational structures are all in alignment with the Organizational ICT strategy.</p> <p>(ii) Mission ICT units develop their work plans in response to strategic guidance from Headquarters, mission mandates and operational imperatives. Missions are discrete programmatic entities. As such, ICTD monitors the actions taken by missions in respect to strategic guidance. While the elements of their work programme related to operational imperatives must be executed in accordance with policies and standards established by United Nations Headquarters, they are not subject to monitoring by DFS/ICTD.</p> <p>iii) The establishment of an ICT risk management framework falls within the purview of OICT. In accordance with paragraphs 35 (i) and (j) of the information and communications strategy for the United Nations Secretariat (A/62/793) dated 9 April 2008, OICT is responsible for among others to: (a) oversee the assessment and management of ICT risks for the Organization; and (b) develop and maintain the information security policy of the</p> |

| | | | | | | |
|----|--|-----|--------------------|----------------|------------------------------|--|
| | | | | | | <p>Organization and monitor compliance across organizational units.</p> <p>Paragraph 46 of the report notes that OICT would complete a comprehensive information security framework by June 2011. In the absence of the Organization-wide framework or any specific security plans and guidance, DFS developed a departmental ICT security framework and supporting high-level policies in 2009 and the implementation is being conducted in a phased approach taking into account the risk based priorities as well as existing capacities in field missions. DFS has established mechanisms to monitor the effectiveness of ICT risk management in peacekeeping missions through the various ICT policy directives as well as the ICT organization structure to facilitate effective and timely monitoring of ICT risks in peacekeeping missions. The revised DPKO/DFS Risk Assessment Policy and the standard operating procedures related to ICT Security Governance and Management Structure are in the final stages of approval, copies of which were provided to OIOS.</p> <p>Based on the above explanation, we request deletion of this recommendation in the final report.</p> |
| 25 | DFS/ICTD should: (a) facilitate the establishment and functioning of Local ICT Committees at the mission level and act as a central coordinating body on all ICT matters; and (b) establish monitoring mechanisms to ensure that peacekeeping missions comply with the Organization's policies and standards for approving business cases. | Yes | Important (Medium) | Director, ICTD | 4 th Quarter 2011 | DFS/ICTD accepts the recommendation and will reiterate the guidance provided to peacekeeping missions on the establishment of ICT management structures and local ICT review committees and engage with missions periodically to ensure that no unsanctioned ICT development activities are undertaken. |

| | | | | | | |
|----|---|---|-----------------------|-------------------|------------------------------|--|
| 31 | <p>DFS/ICTD should: (i) coordinate a comprehensive review across all peacekeeping missions to determine the need for future support and maintenance of locally developed applications with reference to the planned implementation of the new ERP/UMOJA, Inspira Talent Management, Customer Relationship Management and Enterprise Content Management; (ii) determine the need for extending the scope of Field Support Suite; and (iii) facilitate security and availability assessments for the locally developed applications that will not be replaced by the Field Support Suite.</p> | <p>(i) No (ii) Yes (iii) No</p> | Important (Medium) | Director, ICTD | 4 th Quarter 2014 | <p>DFS accepts the second part of the recommendation in paragraph 31.</p> <p>(i) Beginning with its 2008/2009 ICT Guidance (“CITS Vision”) and repeated in subsequent yearly strategic guidance to the field, DFS/ICTD has consistently directed field missions not to undertake the development or transfer of local applications that conflict with the enterprise initiatives of the Organization (ERP, Talent Management, CRM, Fuel/Rations and ECM). DFS/ICTD also reminded missions in a facsimile dated 4 November 2009 (copy attached) to “...control the demand for development of new applications or transfer of existing applications between missions.” The purpose of these directives was to limit the investment in new development work that was redundant and/or could complicate the implementation of enterprise systems.</p> <p>(ii) The development and implementation of the Field Support Suite (FSS) was conducted in coordination with the UMOJA Team which sees FSS deployment as an effective mechanism to consolidate data and processes in the field. The implementation of FSS modules to all field missions is underway and scheduled for completion in 2012. Its implementation will result in the decommissioning of local systems that are currently being used to perform similar functions. Local CITS management is kept informed of the enterprise and FSS deployment schedules so that they can adjust the required support and maintenance for local applications accordingly. The scope of the FSS is being extended to meet the business needs of the field and the selection of enhancements and additional modules have been planned in alignment with the Global Field support Strategy as well as through engagement of Headquarters and mission management. FSS is also under consideration as a front end tool to facilitate the data collection and conversions required for UMOJA and IPSAS implementation.</p> |
|----|---|---|-----------------------|-------------------|------------------------------|--|

| | | | | | | |
|----|--|-----|--------------------|-----|-----|--|
| | | | | | | <p>(iii) In the absence of an Organization-wide solution for ICT risk, governance and compliance, ICTD initiated the purchase of a Governance, Risk and Compliance (GRC) tool to improve IT security posture, ICTD's capability to effectively identify and address ICT security risks, improve compliance with security policies and standards and enhance field missions' capabilities to more effectively address the constantly growing number of threats as well as sophisticated malware threats. Paragraph 55 of the report notes that OICT is in the process of working on "the feasibility of an E-GRC platform and developing a proof of concept". ICTD will collaborate with OICT on this enterprise initiative. Please see further comments on the recommendation in paragraph 18 (iii) above.</p> <p>Based on the above explanation, we request deletion of part (i) and (iii) of the recommendation in the final report.</p> |
| 38 | DFS/ICTD, in coordination with OICT, should develop and implement an ICT threat catalog and risk assessment process, and establish mechanisms for monitoring the effective functioning of ICT risk management in the peacekeeping missions. | N/A | Important (Medium) | N/A | N/A | <p>DFS suggests that this recommendation should be amended and redirected to OICT.</p> <p>The implementation of this recommendation is dependent on establishment of Organization-wide solution for ICT risk. Please see our comments on the recommendation in paragraph 18 (iii) above.</p> |
| 47 | DFS/ICTD should develop an ICT security plan, defining the requirements of investments in services, staffing, training, software and hardware to achieve an acceptable global security standard across all peacekeeping missions in alignment with its ICT security framework. | N/A | Important (Medium) | N/A | N/A | <p>DFS suggests that this recommendation should be amended and redirected to OICT.</p> <p>Paragraph 46 of the report states that "OICT will complete a comprehensive information security framework by June 2011 All Departments, Offices away from Headquarters and Regional Commissions' ICT Units will initiate information security discussions with their local ICT units, with a view to advancing business ownership of risk and cost mitigation". DFS/ICTD will develop departmental security plans following the receipt of the</p> |

| | | | | | | |
|----|---|--------------------|-----------------------|-------------------|------------------------------|--|
| 56 | DFS/ICTD should: (i) ensure that its application for governance, risk and compliance (GRC) is supported by a documented business case in accordance with the established ICT project management procedures; and (ii) implement mechanisms for monitoring the compliance of peacekeeping missions with ICT policies. | (i) No (ii) Yes | Important (Medium) | Director, ICTD | N/A | <p>global ICT security plan and in the absence of such a plan, DFS/ICTD will continue the phased implementation of the Departmental security framework within its available capacities. Please see further comments on the recommendation in paragraph 18 (iii) above.</p> <p>(i) In accordance with OICT's portfolio management, a business case is not required for projects under \$250,000. Since the cost of the GRC project is below the threshold of \$250,000, the procedure followed by ICTD was in compliance with the above quoted guidance. The link is attached below for easy reference: http://iseek.un.org/webpageprint1630_1.asp?dept=1630#.</p> <p>Based on the above explanation, we request deletion of part (i) of the recommendation in the final report.</p> <p>(ii) The implementation of the second part of the recommendation is dependent on the development of an E-GRC platform by OICT referred to in the recommendation in paragraph 31 (iii) above.</p> |
| 64 | DFS/ICTD should consider completing the disaster recovery plans of all peacekeeping missions by including: (i) the list of mission critical applications; (ii) the definition of recovery time and point objectives; (iii) alignment with the missions' business continuity plans; and (iv) a standard template for reporting disaster recovery test results. | Yes | Important (Medium) | Director, ICTD | 4 th Quarter 2011 | <p>DFS is in the process of developing guidance which will be communicated to the field missions in the fourth quarter of 2011.</p> |

ANNEX II
OPPORTUNITIES FOR IMPROVEMENT

Assignment No. AT2011/615/01 - Audit of ICT governance and security management in peacekeeping missions

| Para. no. | Recommendation | Client comments |
|------------------|--|---|
| 35 | DFS/ICTD could improve the awareness of ICT-related policies, standard operating procedures and guidelines by publishing them in the intranet web site of DFS/DPKO containing the peacekeeping policy framework. | Policies, SOPs and guidelines which are still in draft form have to be reviewed and finalized before they are posted on the DFS/DPKO intranet. However ICTD conducts security awareness programmes and advises all missions of current documentation that are posted on the DFS/ICTD webpage. |
| 52 | DFS/ICTD could improve the monitoring process of ICT security in peacekeeping missions by establishing reporting requirements, frequency and metrics. | Please see DFS comments in the recommendation in paragraph 18 (iii) above |