

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

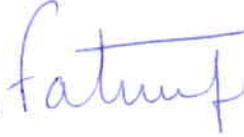
OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE  
INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

TO: Mr. Vijay Nambiar,  
A: Chef de Cabinet  
Executive Office of the Secretary-General

DATE: 22 February 2010

REFERENCE: IAD: 10- 00086

FROM: Fatoumata Ndiaye, Director  
DE: Internal Audit Division, OIOS



SUBJECT: **Assignment No. AT2008/510/01 – Horizontal audit of data privacy in the United Nations Secretariat**  
OBJET:

**The Executive Office of the Secretary-General should ensure that adequate controls are implemented for the security of the systems and applications in use.**

1. I am pleased to present the report on the above-mentioned audit which was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. While cross-cutting issues related to data privacy in the UN Secretariat have been documented in a separate report, this memorandum addresses issues specific to the Executive Office of the Secretary-General.
3. In order for us to close the recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e. recommendation 1), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

## EXECUTIVE SUMMARY

### Horizontal audit of data privacy in the United Nations Secretariat

OIOS conducted an audit of data privacy across the United Nations Secretariat. The overall objective of the audit was to determine whether the Secretariat has adequate controls in place to protect the confidentiality and integrity of sensitive information related to employees, representatives of Member States, and other individuals. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The cross-cutting issues identified during the course of the audit have been documented in a separate audit report (IAD:09-02378). This report addresses the risks and controls specific to the Executive Office of the Secretary-General (EOSG).

Two new information systems are being installed in EOSG to support the scheduling and document management processes. In consideration of the sensitivity of data and information stored in these applications, OIOS recommended the implementation of adequate physical and logical safeguards to ensure their confidentiality and integrity.

## **I. INTRODUCTION**

1. The Office of Internal Oversight Services (OIOS) conducted an audit of data privacy at the United Nations Secretariat. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing .
2. Data privacy refers to the right of individuals to control the collection and use of personal information about themselves. The Black's Law Dictionary defines it as "a private person's right to choose to determine whether, how, and to what extent information about oneself is communicated to others". It has not been formally defined by the United Nations Secretariat.
3. Comments made by the Executive Office of the Secretary-General (EOSG) are shown in *italics*.

## **II. AUDIT OBJECTIVES**

4. The main objectives of the audit were to assess whether:
  - (a) A governance system is in place to manage privacy of data;
  - (b) The Secretariat has defined what data should be considered sensitive, with particular reference to privacy of data, per ST/SGB/2007/6 on Information sensitivity, classification, and handling; and
  - (c) Adequate controls are in place for the protection of data privacy.

## **III. AUDIT SCOPE AND METHODOLOGY**

5. The audit covered the current policies, procedures, working practices and systems in EOSG.

## **IV. AUDIT FINDINGS AND RECOMMENDATIONS**

Security of systems and applications used by EOSG

6. The audit review conducted by OIOS in EOSG included the activities of the following units:
  - i) Scheduling Office;
  - ii) Policy Unit;
  - iii) Central Registry;
  - iv) Political Unit;
  - v) Office of the Chef de Cabinet;
  - vi) Executive Office; and
  - vii) ICT Support Unit.

---

7. As a result of the review conducted in EOSG, OIOS identified two initiatives, supported by OICT, that are relevant for the purpose and scope of this audit. These initiatives pertained to the following applications:

a) The Secretary-General's Relationship Management (SGRM), a web-based application built on a customer relationship management (CRM) solution, which went live on 15th July 2008, in the EOSG office. The application is used by the Scheduling Office and Front Office to consolidate scheduling tasks, files, and communications. It contains information on SG's meetings, events, trips, contacts and organizations, stored centrally and accessed in a secure manner; and

b) The Correspondence Management Application (eCMA), being developed to manage EOSG correspondences to:

- Capture correspondence at origin;
- Enable simultaneous distribution of correspondences;
- Manage correspondences throughout their lifecycle;
- Digitally preserve correspondences and their context;
- Offer collaborative authoring for correspondences;
- Create correspondence alerts based on their importance;
- Increase speed and quality of search and retrieval;
- Improve document security;
- Improve reporting capability; and
- Improve the business processes in creating and managing correspondence.

8. In consideration of the sensitivity of data and information stored in these applications, it is imperative that adequate physical and logical safeguards are in place to ensure their confidentiality and integrity.

### **Recommendation 1**

**(1) The Executive Office of the Secretary-General should request the Office of Information and Communications Technology to ensure that the SGRM and eCMA applications are secured with physical and logical controls, including: (a) "audit event logging" mechanisms at the application and operating system levels; and (b) encrypted transmission for remote connectivity.**

9. *EOSG accepted recommendation 1 and stated that the SGRM and eCMA are secure, and that the project teams working with OICT are in the process of retroactively defining the information security requirements and determining the specific security controls that need to be implemented and verified. Recommendation 1 remains open pending submission to OIOS of evidence documenting the definition and implementation of the security requirements of SGRM and eCMA applications.*

## V. ACKNOWLEDGEMENT

10. We wish to express our appreciation to the Management and staff of EOSG for the assistance and cooperation extended to the auditors during this assignment.

cc: Mr. Choi Soon-hong, Assistant Secretary-General, Chief Information Technology Officer  
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors  
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit  
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management  
Mr. Byung-Kun Min, Special Assistant to the USG, OIOS  
Ms. William Petersen, Chief, New York Audit Service, OIOS

### CONTACT INFORMATION:

#### **DIRECTOR:**

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,  
e-mail: [ndiaye@un.org](mailto:ndiaye@un.org)

#### **ACTING DEPUTY DIRECTOR:**

Gurpur Kumar: Tel: +212.963.5920, Fax: +1.212.963.3388  
e-mail: [kumarg@un.org](mailto:kumarg@un.org)

#### **CHIEF, NEW YORK AUDIT SERVICE:**

William Petersen: Tel: +1.212.963.3705, Fax: +1.212.963.3388,  
e-mail: [petersenw@un.org](mailto:petersenw@un.org)

## STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
1	The Executive Office of the Secretary General should request the Office of Information and Communications Technology to ensure that the SGRM and eCMA applications are secured with physical and logical controls, including: a) “audit event logging” mechanisms at the application and operating system level; and b) encrypted transmission for remote connectivity.	Information Resources	High	O	Submit to OIOS documented evidence of the security requirements defined and implemented for the SGRM and eCMA applications.	Not provided

1. C = closed, O = open

2. Date provided by the Executive of Office of the Secretary-General.