

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. Shaaban Muhammad Shaaban,
A: Under-Secretary-General
Department of General Assembly and Conference
Management

DATE: 21 December 2009

REFERENCE: IAD: 09- **03227**

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



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

OBJET:

The Department of General Assembly and Conference Management should ensure that adequate controls are implemented for the security of the "Accreditation Database", and the sharing of data with third party entities.

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 Department of General Assembly and Conference Management.

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., recommendations 1 and 2), 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 Department of General Assembly and Conference Management (DGACM).

DGACM maintains an "Accreditation Database" to process and store data pertaining to the accreditation of diplomatic personnel and support staff of permanent/observer missions, their dependants and household employees. Considering the sensitivity of data processed and stored in this database, OIOS recommended: (a) the implementation of adequate logical access controls to ensure their confidentiality and integrity; and (b) the establishment of adequate procedures to regulate the sharing of this data with third party entities.

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 Department of General Assembly and Conference Management (DGACM) 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 DGACM.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. DGACM – Protocol and Liaison Service (PLS)

Absence of adequate controls and procedures to regulate access to the "Accreditation Database"

6. The portfolio of services provided by PLS include: a) The registration of all diplomatic personnel and support staff of permanent/observer missions, their dependants and household employees, and to provide them with proper United Nations building passes, to approve applications for parking decals, to process requests for diplomatic privileges and immunities for diplomatic personnel of permanent missions, and to maintain and update files with relevant data on all the members of the permanent/observer missions; and b) To accredit members of

governmental or intergovernmental delegations, representatives of specialized agencies, and associate members of regional commissions.

7. The data collected by PLS were stored in the "Accreditation Database" hosted in a web portal of DGACM that was accessible by all PLS staff members and technical programmers of the Information and Communication Technology Section (ICTS). In this regard, however, OIOS noted the absence of defined criteria and adequate controls and procedures to regulate access to the database.

Recommendation 1

(1) The Department of General Assembly and Conference Management should develop a logical access control policy and implement control procedures to regulate access to the "Accreditation Database" during the various steps followed for collecting, processing, storing, and retrieving data.

8. *DGACM accepted recommendation 1 and stated that PLS has effective controls in place to regulate access to its accreditation database. PLS agrees to incorporate its current practices into a written logical access control policy document, outlining the various steps followed for collecting, processing, storing, and retrieving data. Recommendation 1 remains open pending submission to OIOS of evidence documenting the logical access control policy and procedures to regulate access to the "Accreditation Database".*

Lack of procedures for the disclosure of personal data with third party entities

9. PLS shared data with third parties (i.e. Diplomatic missions) for completion and verification of data pertaining to the registration and accreditation process. However, PLS did not have a policy or terms of reference regulating the sharing of personal data with third parties.

Recommendation 2

(2) The Department of General Assembly and Conference Management, in collaboration with the Office of Legal Affairs, should develop a protocol to regulate the disclosure of personal data to third party entities.

10. *DGACM accepted recommendation 2 and stated that PLS applies strict procedures and controls prohibiting disclosure of personal data to third party entities. The sole recipient of such data is the Permanent Mission of the United States of America to the United Nations, for the sole purpose of effectively facilitating the implementation - and within the strict purview of the relevant provisions contained in - the Agreement between the United Nations and the United States of America regarding the Headquarters of the United Nations (A/Res/169 (II), dated 31 October 1947, Article IV). PLS agrees to write a protocol regulating disclosure of personal data to third party entities. Recommendation 2 remains open pending submission to OIOS of evidence documenting the protocol regulating the disclosure of data to third party entities.*

V. ACKNOWLEDGEMENT

11. We wish to express our appreciation to the Management and staff of the Department of General Assembly and Conference Management for the assistance and cooperation extended to the auditors during this assignment.

cc: Ms. Angela Kane, Under-Secretary-General, Department of Management
Ms. Patricia O'Brien, Under-Secretary-General, Office of Legal Affairs
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 Bamuwamye, 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:

ACTING DIRECTOR:

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,

e-mail: ndiaye@un.org

ACTING DEPUTY DIRECTOR:

Gurpur Kumar: Tel: +212.963.5920, Fax: +1.212.963.3388

e-mail: 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

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/ O ¹	Actions needed to close recommendation	Implementation date ²
1	The Department of General Assembly and Conference Management should develop a logical access control policy and implement control procedures to regulate access to the "Accreditation Database" during the various steps followed for collecting, processing, storing, and retrieving data.	Information Resources	High	O	Submit to OIOS documented evidence of the policy and procedures developed for regulating access to the Accreditation Database.	1 September 2009
2	The Department of General Assembly and Conference Management, in collaboration with the Office of Legal Affairs, should develop a protocol to regulate the disclosure of personal data with third party entities	Governance	High	O	Submit to OIOS documented evidence of the protocol developed to regulate the disclosure of personal data by the Protocol and Liaison Service to third party entities.	1 September 2009

1. C = closed, O = open

2. Date provided by the Department of General Assembly and Conference Management in response to recommendations.