UNITED NATIONS DISPUTE TRIBUNAL

Case No.:	UNDT/NY/2010/054
Judgment No.:	UNDT/2011/069
Date:	12 April 2011
Original:	English

Before: Judge Marilyn J. Kaman

Registry: New York

Registrar: Santiago Villalpando

MORIN

v.

SECRETARY-GENERAL
OF THE UNITED NATIONS

JUDGMENT

Counsel for Applicant:
Colleen M. Rohan

Counsel for Respondent:
Melissa Bullen, ALS/OHRM, UN Secretariat

Notice: The format of this judgment has been modified for publication purposes in accordance with Article 26 of the Rules of Procedure of the United Nations Dispute Tribunal.

Introduction

1. The Applicant appeals against a 4 January 2010 decision of the Secretary-General denying him access to certain information that he contends is needed to prepare an informed and adequate response to allegations of misconduct that were brought against the Applicant on 29 June 2009.

2. Access to this information was initially denied by the Organization on the ground that the requested information is highly confidential and sensitive in nature. Under his application, the Applicant requested the Tribunal to issue an order directing that he be given access to material, as specified in an annex to his application.

3. As will be outlined below, the parties have agreed that the Applicant and/or his Counsel be allowed to have access to the requested information, although the parties disagree on the exact conditions governing access to and review of the requested information. The Applicant agrees with each element of the Respondent's latest proposed final access conditions ("Proposed Final Access Conditions") except for one—whether notes taken by Counsel for the Applicant during her review of the information (including attorney work product) could be taken away from the secure viewing room.

Issue

4. The issue to be addressed by the Tribunal in the present Judgment is to be defined as follows: do the Proposed Final Access Conditions correctly balance the Respondent's interest in protecting confidential information to ensure organizational security against the Applicant's interest in presenting a full defense to the disciplinary charges that have been filed against him?

Facts

5. On 1 January 2006, the Applicant began working as a P-4 level Desk Officer, at the West Africa Desk, Department of Safety and Security ("DSS"), United Nations Headquarters. The Applicant became Officer-in-Charge, West Africa Desk, DSS, in May 2007 and was employed in that capacity in December 2007.

6. On 19 June 2008, in response to the 11 December 2007 attack against the United Nations House in Algiers, the Secretary-General established an Independent Panel on Accountability ("Panel") with a mandate of, *inter alia*: (a) identifying United Nations officials and offices concerned with United Nations operations in Algiers; (b) making findings regarding any acts or omissions of officials; and (c) making recommendations as to whether disciplinary or administrative proceedings should be initiated.

7. On 21 September 2008 the Panel completed its work and delivered a report ("IPA Report") to the Secretary-General.

8. By memorandum dated 15 June 2009 from Mr. Gregory Starr, Under-Secretary-General, DSS, 81 specific texts of the IPA Report were recommended for redaction for general reasons relating to organizational security.

9. The recommended redactions were incorporated into the IPA Report ("Redacted IPA Report"), which was then made available for review by staff members against whom administrative or disciplinary proceedings were recommended by the IPA Panel, and their counsel. This review was to take place under special secure arrangements.

10. By memorandum dated 29 June 2009 ("Charge Letter"), the Office of Human Resources Management ("OHRM") advised the Applicant that disciplinary proceedings would be instituted against him. The Applicant was informed that he was being charged with "having failed to properly fulfill [his] key functions of managing and supervising the West Africa Desk, in particular by failing to act

following the analysis presented in the TRU [Threat and Risk Assessment Unit] assessments and upon receipt of the October 2007 SRA [Security Risk Assessment] in contravention of Staff Rule 1.2(b)". The Applicant was requested to provide comments in response to the Charge Letter and was informed of his right to counsel.

11. The Applicant and his Counsel were advised that arrangements would be made for them to access the Redacted IPA Report. One condition of the review of the Redacted IPA Report was that the Applicant and his Counsel were to sign a strict Confidentiality Undertaking ("Confidentiality Undertaking", reproduced in Confidential Annex C to the Application).

12. Under Counsel's Confidentiality Undertaking:

a. Counsel was permitted to review the copy of the redacted IPA Report in a designated, secure room, at designated times;

b. Counsel was prohibited from: (i) making copies of, or from, the IPA Report; (ii) bringing into the reviewing room any laptops or recording devices; and (iii) altering, modifying, varying, destroying or removing the IPA Report from the reviewing room;

c. Counsel acknowledged that the IPA Report contained strictly confidential information generally relating to organizational security;

d. Counsel made four undertakings: (i) not to disclose, without the Organization's prior written consent, any information contained in the IPA Report to any person except the Applicant, and not to disclose any notes that Counsel or her client may take from the IPA Report, nor any comments prepared in that respect; (ii) to take all steps necessary to ensure that no person other than the Applicant gains access to the information made available to Counsel; (iii) to notify the Organization immediately if Counsel learns that a person not duly authorized has gained access to the information, such notification to include the identity of the person; and (iv) not to use the

information contained in the IPA Report for any purpose other than for the preparation of the submission to the Organization only of the Applicant's comments on the findings and recommendations of the IPA Report that relate to the Applicant and/or on the allegations of misconduct which have been filed;

e. Counsel acknowledged that in the event of breach of one of the obligations set forth, action may be taken against Counsel by the Organization including, without limitation, for wrongful disclosure and breach of confidentiality.

13. On 7 October 2009, Counsel for the Applicant requested from the Respondent certain documentation that was missing from or had been redacted from the original IPA Report.

14. By letter dated 18 November 2009, the Respondent informed the Applicant that the Further Information would not be disclosed in full to the Applicant. This letter did however communicate arrangements which were being made to have some of the Further Information made available to the Applicant's Counsel.

15. On 3 December 2009, the Applicant filed a request for management evaluation of the decision not to release the Further Information to the Applicant and his Counsel. On 4 January 2010, the Respondent, through the Management Evaluation Unit's response, upheld this decision.

16. On 17 February 2010, the Applicant filed an application with the Dispute Tribunal to seek an order that the Applicant be given access to the Further Information in full.

17. On 29 March 2010, the Respondent filed his reply, and outlined the measures already taken by the Respondent to ensure that the IPA Report and supporting documentation remained strictly confidential (Respondent's reply, para. 29, ("Paragraph 29 Measures")).

18. The Paragraph 29 Measures were outlined, as follows:

a. The staff members assigned with the responsibility of the day-to-day conduct of the administrative and disciplinary proceedings recommended by the Panel have been located in a secure space to which access by other staff members, including those handling other disciplinary matters as part of their normal functions, are barred;

b. The computers in the secure space are not connected to other computers in OHRM by means of a shared drive;

c. Various parts of the IPA Report and its supporting documentation identified by DSS have been redacted;

d. The normal working methods used by staff members working on these cases have been restricted—although all disciplinary cases are treated confidentially. Additional restrictions employed in the handling of the Applicant's case and the cases of the other staff members in this matter reflect the highly sensitive nature of the information involved;

e. The Redacted IPA Report and supporting documents, which were made available to the staff members subject to administrative and disciplinary proceedings, were made available only in secure offices with 24-hour video surveillance and staff members who were charged or subject to administrative proceedings, and their counsel, were prohibited from bringing their own computers when reviewing the documentation in order to avoid the risk of the information being copied. Other precautions taken are set out in the Charge Letter;

f. The Respondent, in providing the Applicant and Counsel for the Applicant with copies of the Redacted IPA Report and supporting documentation, made arrangements for the documentation to be hand-delivered to [the Applicant's office] in Rome on one occasion, and to [the

Applicant's Counsel's office] in The Hague on two occasions. It is to be noted that the sealed documentation stayed in the hands of the couriers, who were staff members of the United Nations or the International Criminal Tribunal for the former Yugoslavia ("ICTY") at all times, that the non-OHRM couriers signed confidentiality undertakings and that all couriers were provided with letters stating that the sealed package they were carrying was inviolable under the law relating to the privileges and immunities of the United Nations in order to respond to inquiries by local authorities; and

g. A record was kept of each occasion when a staff member who was charged or subject to administrative proceedings, and/or his counsel, reviewed the redacted IPA Report and supporting documentation.

Procedural background

19. By Order No. 125 (NY/2010) of 21 May 2010, this Tribunal (Judge Ebrahim-Carstens) ordered the Respondent to file with the Tribunal, on an *ex parte* basis, the Further Information sought by the Applicant, upon which the Tribunal would review the Further Information to determine whether the documents were relevant and capable of assisting the Applicant's case. The Tribunal determined that it would thereupon advise the Respondent, again on an *ex parte* basis, which documents within the Further Information the Tribunal had identified as potentially relevant and then allow the Respondent an opportunity to argue his contention as to why the documents should, nevertheless, not be disclosed to the Applicant.

20. Following a number of time extensions, on 31 August 2010, the Respondent filed the Further Information in full under seal with the Registry, in compliance with Orders Nos. 125, 181 and 203 (NY/2010), together with a motion seeking the maintenance of the confidentiality of the documents.

21. In order to assist the Tribunal in making its rulings regarding the Further Information sought by the Applicant, on 22 September 2010 the Tribunal held a case management hearing before Judge Kaman, at which time Counsel for both the

Applicant and the Respondent were present, as well as two officials of DSS. In advance of this hearing, the parties had been advised by Order No. 238 (NY/2010) of questions in relation to which the Tribunal sought background information. The parties were notified that this information was to be of a background nature only, and not considered as tendered evidence.

22. Following the 22 September 2010 case management hearing, which the Tribunal found to be most instructive, and following the Respondent's production to the Applicant of some documents contained within the Further Information, the parties conferred with one another with a view to reaching an agreement on the Applicant's request for production of the remainder of the Further Information. The parties were unable to reach a complete agreement on how to resolve the Applicant's access to the Further Information.

23. On 3 December 2010, the Respondent filed with the Tribunal a submission outlining a procedure by which he proposed to provide the Applicant full access to the Further Information, subject to certain conditions in addition to those set forth in the Confidentiality Undertaking and in the Paragraph 29 Measures. The Respondent stated that:

> [I]n the interests of the expeditious resolution of the disciplinary proceedings concerning the Applicant, the Respondent has considered carefully what further steps [he] could reasonably take in order to satisfy the Applicant, while complying with [his] obligation to protect [his] staff and their interests.

This submission was initially filed on an *ex parte* basis, but, in accordance with Order No. 322 (NY/2010), it was disclosed to the Applicant in order that his response could be sought.

24. On 8 December 2010, the Applicant filed a response to the Respondent's 3 December 2010 additional proposal for access to the Further Information. The Applicant agreed with all points of the Respondent's proposal (outlined below),

excepting the requirement that "no notes or attorney work product of any kind can be removed from the room in which the [Further Information] is reviewed".

25. At the *ex parte* hearing of 8 December 2010, the Respondent further clarified to the Tribunal his additional proposal for access to the Further Information, following which the Applicant was notified of this proposal by Order No. 322 (NY/2010), and given an opportunity to respond to it. The parties thereafter each made further submissions to the Tribunal regarding this proposal.

26. On 13 January 2011 the Tribunal issued Order No. 6 (NY/2011), which stated, *inter alia*:

> 3. The Parties' submissions generally reflect an agreement for the Applicant to be given access to all of the Further Information he seeks. However, there is an issue of contention between the Parties relating to the conditions attaching to this access. Specifically, the Applicant objects only to the condition of access proposed by the Respondent that no notes derived from review of the Further Information and no "attorney work product" would be permitted to be removed from the secure room.
>
> 4. The Applicant says that this proposed condition is unworkable, as it directly interferes with the functioning of his attorney-client relationship, leads to an inequality of arms in the disciplinary proceedings, impacts his Counsel's ethical obligations to her client and is disproportionate, given the history of the litigation in the case. The Respondent disagrees and says that the only prejudice the Applicant will suffer from the proposed condition is one of convenience and is therefore not substantive.
>
> 5. In the submission of 15 December 2010 the Applicant "requests that th[e] Tribunal enter whatever Order it deems to be just and proper". In the submission of 12 January 2011 the Respondent requests the Tribunal "to rule accordingly".
>
> 6. In light of the Parties' submissions, the Tribunal proposes to issue a Judgment ruling on the proposed conditions of access, subject to which the case would be closed. While the following orders are made to allow the Parties an opportunity to respond to this proposal, decisions regarding the conduct and disposal of the case will ultimately be at the discretion of the Tribunal.

27. On 27 January 2011 and 12 February 2011, the Applicant and the Respondent respectively provided their consent to the Tribunal ruling on the proposed conditions of access to the Further Information. With the 12 February 2011 submission, the Respondent provided further particularization of the proposed access measures contained in his 3 December 2010 submission. These measures are detailed below at para. 30 and are those described in this Judgment as the "Proposed Final Access Conditions".

Respondent's submissions

28. The Respondent's principal contentions regarding circumstances for the production of the Further Information are presented first for ease of understanding, and may be summarized as follows:

a. The Respondent has treated the IPA Report and its supporting documentation as being "strictly confidential";

b. In pursuing disciplinary proceedings against the Applicant, the Respondent, consistent with ST/SGB/2007/6 (Information sensitivity, classification and handling), has taken extraordinary measures to ensure that the IPA Report and supporting documentation, due to their sensitivity, remain strictly confidential. The Respondent has gone beyond the use of the minimum standards and has put in place strict controls on access to the information, including but not limited to, the use of dedicated secure space and ICT resources, employment of highly restricted working methods and scrupulous record keeping;

c. Given the nature of the Further Information, the Respondent has significant concerns in relation to its unauthorized disclosure, which concerns are not directed at the Applicant or his Counsel personally, but arise out of a broader need to prevent inadvertent disclosure to the public domain;

d. The Respondent has gone to significant lengths to formulate a proposal that is reasonable and proportionate, and provides the Applicant with full access to the Further Information, while maintaining the obligation to protect United Nations staff;

e. Following the various proposals advanced by the Respondent to resolve the issue of Applicant's and/or his Counsel's access to the Further Information, the proposal submitted by the Respondent is reasonable and satisfies fully the Applicant's right to respond to the allegations against him.

Applicant's submissions

29. The Applicant's principal contentions regarding circumstances for the production of the Further Information may be summarized as follows:

a. Both the Applicant and his Counsel have signed strict confidentiality agreements which absolutely forbid the release of any information obtained in this case;

b. The Applicant does not object to the conditions the Respondent has proposed (in the 3 December 2010 submission), except the condition that the Applicant's Counsel could not take any notes made during review of the documents and tape recordings at issue outside of the room; Counsel for the Applicant also objects to not being permitted to retain her own attorney work product;

c. The original Confidentiality Undertaking remains in effect, namely that all the Further Information must be kept in a locked room, no materials can be copied, scanned or removed from the room, and personal laptops are not allowed in the room; in the case of the Applicant's Counsel, the room in question is kept under constant camera surveillance. The Applicant has already agreed to and worked under these conditions for the dozens of hours

already spent in review of documents that were disclosed as part of the IPA Report;

d. The Applicant has no objection to the addition of a Security Guard in the room, along with the already existing surveillance camera;

e. In reviewing materials to date, however, Counsel for the Applicant has been permitted to place her personal notes on a thumb drive which she has been permitted to remove from the room; Counsel keeps that thumb drive in a locked drawer;

f. Counsel for the Applicant is permitted, under current conditions, to prepare legal documents and to consult with her client outside of the designated room, and has been doing so for the past year;

g. The 3 December 2010 provisions forbid the removal of notes or any attorney work product, including the final written submission to be given to OHRM in response to the Charge Letter. The 3 December 2010 provisions require that the submission to OHRM be prepared in the designated room and also require an "un-networked" computer—a provision which appears to preclude access to legal or other research online while the final work product is in the process of production;

h. Since Counsel for the Applicant is located in The Hague and the Applicant is located in Rome, these conditions effectively prevent the Applicant and his counsel from consulting on the work product while it is being produced and, it appears, even after it is produced. The Applicant is required to travel around the world dealing with humanitarian crises when and as they arise, and is not in a position to be physically present with Counsel in The Hague at those times when Counsel is available to work on his case;

i. The new conditions—no removal of notes from the room and no removal of work product from the room—constitute a direct and substantive

interference with the attorney-client relationship, prevent Counsel for the Applicant's ability to safeguard her own attorney work product, and are unwarranted.

The Proposed Final Access Conditions

30. The Proposed Final Access Conditions for access to the Further Information, as proposed to by the Respondent, are as follows:

a. All of the Further Information (including the 15 tape recordings of witnesses requested by the Applicant) will be made available in a dedicated secure room, to be provided by ICTY, in The Hague, where the Applicant's Counsel is physically located;

b. The review of the Further Information will take place, in the secure room, with 24-hour video surveillance (video only with no sound recording), in the presence of an ICTY Security Officer, who will be in the room with the Applicant and/or his Counsel at all times;

c. Counsel for the Applicant will have access to a telephone in the secure room from which to call her client and other parties, at liberty, which calls will be unrecorded;

d. The Respondent will take such steps as necessary to ensure that, despite the video recording of the secure room, the Applicant's Counsel could work and consult with her client and others without her work being observed (while she was present or otherwise). In this regard, the telephone, computer screen and keyboard can be situated out of view of the video surveillance;

e. Counsel for the Applicant will be permitted to bring her own portable electronic storage device (referred to as a "thumb drive" in the submissions) into the secure room for the purpose of transferring documents to the computer in the secure room. However, any and all material created by the

Applicant and/or his Counsel, while in the room, or brought into the room, shall remain in the room—no item containing information relating to the Further Information is to be removed from the secure room, including any notes, documents or material saved on a thumb drive or similar created by the Applicant and/or his Counsel during the course of the review;

f. The Applicant and/or his Counsel will be required to use a "clean", "stand-alone" computer (that is, a non-networked computer) on which to prepare his response; the resultant work product of which shall not be removed, by thumb drive or otherwise;

g. Counsel for the Applicant will be permitted to leave notes or other materials in the secure room in a secure container which can only be opened by her. To this end, the Respondent will provide any or all of the following:

> i. An encrypted USB thumb drive, accessible only by a password created by Counsel for the Applicant, upon which her work product could be stored. This would offer, *inter alia*: full privacy, as 100 percent of stored data is protected by 256-bit Advanced Encryption Standard hardware-based encryption; advanced security, as the drive locks down and reformats after 10 intrusion attempts; and enforced password protection, as the password is user-set with minimum characteristics to prevent unauthorized access;
>
> ii. A removable hard drive, upon which Counsel's work product could be stored, which would be quickly and easily removable from the "standalone" computer; and
>
> iii. A safe, in which either a removable hard drive or encrypted USB thumb drive or a computer, or all three, could be stored. Counsel for the Applicant would be provided with the only existing sets of keys to the safe (in which case Counsel would accept the sole custody and

responsibility for the safekeeping of the keys and their return at the conclusion of the case);

h. In order to give the Applicant the opportunity to access the documents and to consult with his Counsel, the Respondent is prepared to bear the cost of one roundtrip airfare between Rome (where the Applicant is serving) and The Hague and up to a maximum 14 days' Daily Subsistence Allowance in The Hague. The Applicant would himself personally be able to enter the secure room under the same conditions as his Counsel;

i. The secure room and the contents thereof, including Counsel for the Applicant's "work product", will be available to Counsel for the Applicant, subject to the conditions herein, if necessary, 24 hours a day, seven days a week (with one day's notice required for weekday access, and two days' notice for weekend access);

j. Counsel for the Applicant will be given a reasonable opportunity in terms of the time period permitted to her to prepare her client's response to the allegations of misconduct, which period is, within reason, negotiable with the Respondent (the time period in which staff members are requested to respond to allegations of misconduct is usually two weeks, but the Respondent would be prepared to allow "substantially longer" than this);

k. Arrangements will be made for the secure and in-person transmittal of the final work product to OHRM at Headquarters in New York;

l. The provision of the Further Information will also be subject to the terms of the existing confidentiality agreement between the Organization and Counsel for the Applicant;

m. The Respondent is prepared to take whatever steps are reasonably open to him to make the review process as comfortable and convenient as possible for the Applicant and his Counsel. In addition to making the secure

room available on demand, 24 hours a day, seven days a week, ICTY will provide other comforts and conveniences such as a refrigerator, microwave, kettle and any other items reasonably requested. The Respondent will also provide the Applicant and/or his Counsel with any other reasonable resources or assistance as required, such as additional thumb drives;

n. As noted above, the Applicant agrees to the imposition of all of the Proposed Final Access Conditions, save for the condition that no notes derived from the review of the Further Information and no "attorney work product" can be removed from the secure room ("the Contested Condition of Access").

Consideration

31. The Respondent asks the Tribunal to enter an order specifying the circumstances under which the Applicant and his Counsel have access to the Further Information and prepare court documents based on it—that is, an order imposing the Contested Condition of Access.

32. Article 18.2 of the Tribunal's Rules of Procedure gives the Tribunal the power to "order the production of evidence for either party at any time and may require any person to disclose any document or provide any information that appears to the Dispute Tribunal to be necessary for a fair and expeditious disposal of the proceedings". Article 18.4 of the Rules of Procedure makes clear that the Tribunal is empowered to consider the type of order sought by the Respondent, specifying that, at the request of either party, the Tribunal "may impose measures to preserve the confidentiality of evidence, where warranted by security interests or other exceptional circumstances".

33. Any judicial determination must weigh the competing interests of the parties, the exigencies of the case, and notions of due process and fair trial. An order concerning the production of any document over which confidentiality is sought

should be specifically tailored to meet the necessities of each case, so that the order is neither unduly restrictive nor impermissibly lax.

34. Access to sensitive information in the United Nations is governed by ST/SGB/2007/6. Section 1.2 provides, *inter alia,* that information deemed sensitive shall include: (a) documents whose disclosure is likely to endanger the safety or security of any individual, violate his or her rights or invade his or her privacy (sec. 1.2(b)); (b) documents whose disclosure is likely to endanger the security of Member States or prejudice the security or proper conduct of any operation or activity of the United Nations, including any of its peacekeeping operations (sec. 1.2(c)); and (c) documents covered by legal privilege or related to internal investigations (sec. 1.2(d)). Section 2.1 provides that sensitive information may be classified as "confidential" or "strictly confidential".

35. It bears noting that, in cases where a request for confidentiality is made, the underlying premise to such a request is that the request is legitimate and made in good faith: that the Organization has a *bona fide* belief that the information deserves protection by means of a court order due to its confidentiality and sensitivity. Conversely, any information that has become "stale" would not need protection, for public disclosure in such an instance presumably would not adversely affect safety and security of the United Nations.

36. The Tribunal emphasizes that the Tribunal accepts, for purposes of the present Judgment, the Respondent's contention that the Further Information remains of a sensitive and confidential nature. Given the lapse of time of four years from the December 2007 attack, it might be questioned whether the Further Information has become outdated. The Respondent has not altered its stance as to the strictly confidential nature of the Further Information, and the Tribunal accepts the Respondent's contention regarding the need for protective measures, without evaluating this further and without making an official determination of its accuracy. That issue may arise in other proceedings, but it is not before this Tribunal at this time.

37. The interest of the Respondent in obtaining an order limiting disclosure of confidential information in this case has been stated. Where unauthorized disclosure could reasonably be expected to cause grave damage to the work of the United Nations, the Organization must take steps towards eliminating or minimizing that risk. The events forming the basis for the misconduct charge against the Applicant underscore the necessity of prudent and thoughtful action by the Organization.

38. On the other hand, the Applicant now faces serious disciplinary charges arising from a catastrophic event. Although technically not criminal charges, the misconduct charge of "having failed to properly fulfill [his] key functions of managing and supervising the West Africa Desk, in particular by failing to act following the analysis presented in the TRU [Threat and Risk Assessment Unit] assessments and upon receipt of the October 2007 SRA [Security Risk Assessment]" under Staff Rule 1.2(b) carry overtones of criminal proceedings, where rights attendant to a fair trial attach.

39. Thus, the Applicant avers that the Contested Condition of Access constitutes a direct and substantive interference with the attorney-client relationship, prevents Counsel's ability to safeguard her own attorney work product, and is unwarranted. Counsel for the Applicant in essence makes an argument that the imposition of the Contested Condition of Access would result in an inequality of arms; that is, that he would be unable to prepare or present his case on the same footing as the Respondent.

40. Equality of arms is a concept that has been developed in both domestic and international law. In particular Article 14.1 of the 1966 International Covenant on Civil and Political Rights ("ICCPR") enshrines *inter alia* the principle of equality of all persons before courts and tribunals, and the principle of fair trial (see also, art. 6.1 of the 1950 European Convention on Human Rights ("ECHR") and art. 8.1 of the 1969 American Convention on Human Rights). Although art. 14.1 of the ICCPR puts special emphasis on judicial proceedings of a criminal nature, the Human Rights Committee , in its General Comment No. 31 on "Article 14: Right to equality before

courts and tribunals and to a fair trial" (UN Doc. CCPR/C/GC/32), noted that the principle is not limited to criminal proceedings.

41. In General Comment No. 31, the Human Rights Committee also noted that "[t]he right of equality before courts and tribunals, in general terms, guarantees… [the principles] of equal access and equality of arms, and ensures that the parties to the proceedings in question are treated without any discrimination". The Committee interpreted "equality of arms" as meaning that "the same procedural rights are to be provided to all the parties unless distinctions are based on law and can be justified on objective and reasonable grounds, not entailing actual disadvantage or other unfairness to the defendant". That the concept of a fair hearing in the context of art. 14.1 of the ICCPR and art. 6.1 of the ECHR requires conditions including equality of arms has been confirmed in jurisprudence (see, for example: Human Rights Committee, *Morael v. France,* Communication No. 207/1986, 28 July 1989, UN Doc. CCPR/C/36/D/207/1986; European Court of Human Rights, *Dombo Beheer B.V. v. The Netherlands*, Application No. 14448/88, Judgement of 27 October 1993).

42. International norms and general principles of law may assist the Tribunal in the determination of matters before it (see discussion in *Obdeijn* UNDT/2011/032, citing *Tabari* 2010-UNAT-030, *Muthuswami et al.* 2010-UNAT-034 and *Chen* UNDT/2010/068). In this way, equality of arms may be seen to be an indivisible element of a fair trial, requiring that a fair balance exist between parties involved in litigation. The principle warrants the assurance that each party to a dispute be able to prepare and present his or her case fully and adequately before the court.

43. The Tribunal, then, must ascertain the proper balance to be struck between the competing interests involved in this case. It must decide whether imposing the Contested Condition of Access as part of the Proposed Final Access Conditions would strike a fair balance between allowing the Applicant to properly prepare and present his case, while protecting against the risk of the unauthorized disclosure of the confidential Further Information which would prejudice the Organization's security. The inquiry is significant because it carries important implications about

questions of organizational security and the robustness of the right to a fair trial (including the right to counsel).

44. Some of the factors that the Tribunal should consider in making this type of determination include the following:

a. whether the confidential material is relevant to facts at issue in the proceedings;

b. whether legitimate confidentiality reasons are present;

c. whether measures can be imposed to protect the particular interests at risk;

d. whether the security interests of the Organization require confidentiality, such as accounting, auditing, inspection or investigation systems or procedures or a similar nature;

e. whether the public disclosure might compromise the personal safety of any person or persons;

f. whether exceptional circumstances exist that merit a designation of confidentiality;

g. whether the interests of justice require disclosure; and

h. any other considerations the Tribunal deems relevant to its decision.

45. In the current matter, as noted at paragraph 36, above, the Tribunal accepts the Respondent's contention as to the confidentiality of the Further Information, and with this the risk posed by its unauthorized disclosure. The relevance of the Further Information has already been conceded by the Respondent. The Respondent has agreed to give full access to the Further Information and proposed the Proposed Final Access Conditions, all of which create a large administrative burden and cost on the Organization, but which the Respondent is prepared to bear, as he says they are necessary to protect the Organization's interests. The Contested Condition of Access is the primary condition within the Proposed Final Access Conditions that creates a burden for the Applicant in the preparation of his case.

46. The Tribunal finds that the Proposed Final Access Conditions, including the Contested Condition of Access, result in a fair outcome which balances the interests of justice. While there will be some difficulty for the Applicant (and his Counsel) in the preparation of his case, he will have access to all of the information he seeks, and is to be granted a time period which is reasonable in the circumstances to utilize this information in the preparation of his defence.

47. As a final matter, the Tribunal wishes to express its appreciation to both parties in this matter for the extensive efforts and compromises made in order to work cooperatively with the Tribunal to obtain a just outcome. The parties have assisted the Tribunal and complied at all times with its directions in relation to a particularly sensitive subject matter. The diligent efforts of Counsel and their instructors are duly noted and are to be commended.

Conclusion

48. The Applicant is granted access to the Further Information in accordance with the conditions specified at para. 30 (a)–(m) of this Judgment.

49. The Respondent shall allow the Applicant a reasonable time period (which shall be, at all events, no less than four months from the time the Applicant or his Counsel is first able to view the Further Information) to prepare his response to the Charge Letter.

(*Signed*)

Judge Marilyn J. Kaman

Dated this 12th day of April 2011

Entered in the Register on this 12th day of April 2011

(*Signed*)

Santiago Villalpando, Registrar, New York