

**SECTION M**

**CONFIDENTIALITY SUPPLEMENT TO THE OPCW  
DECLARATIONS HANDBOOK**

**OPCW**

**November, 2008**

---

## Confidentiality Supplement to the OPCW Declarations Handbook

### Introduction

While recognising that a State Party has ultimate authority in designating the classification level and the method of delivery of the information it provides to the Organisation, this Confidentiality Supplement is intended to illustrate for National Authority personnel the concepts presented in the OPCW Policy on Confidentiality (OPOC).

### 1. Determining the level of sensitivity of confidential information

1.1 To ensure the appropriate handling and protection of confidential information provided to or generated by the OPCW, paragraph 1.2 of Part V of the OPOC, states that *“the essential factors to be considered in determining the level of sensitivity of an item of information are as follows:*

- (a) the degree of potential damage which its disclosure could cause to a State Party, any other body of a State Party, including a commercial firm, or to any national of a State Party, or to the Convention or the Organisation; and*
- (b) the degree of potential particular or selective advantage its disclosure could offer to an individual, a State, or any other body, including a commercial firm.*

*These factors correspond to the factors used in determining the confidentiality of information.”*

1.2 Guidelines on the OPCW classification system for confidential information, as specified in paragraphs 1.3 through 1.6 of Part V of the OPOC, state:

*“Based on these guiding factors, and the specific classification criteria set out below, confidential information shall be classified according to the following categories, in increasing order of sensitivity:*

- OPCW RESTRICTED*
- OPCW PROTECTED*
- OPCW HIGHLY PROTECTED*

*Information not falling into any of the above-mentioned categories shall be considered not classified and may be marked appropriately. Information which is not classified will be subject to appropriate protection from release by the Organisation and by States Parties, unless specifically cleared for release in accordance with the separately defined release procedures.*

*The level of protection afforded to confidential information shall be linked to the level of sensitivity as indicated by its classification category. Each State*

---

*Party and the Organisation shall protect OPCW classified information originating both from within the Organisation and from States Parties in accordance with its level of sensitivity as expressed by its classification category.”*

- 1.3 Guidance on the criterion for determining the relevant classification to be applied to information to be submitted to the Technical Secretariat, if so necessitated, is contained in paragraphs 1.7 to 1.18 of Part V of the OPOC and has been included in Annex 1 to this Confidentiality Supplement.
- 1.4 While States Parties have the right to classify any information it provides to the Technical Secretariat, it should be stressed that it is standard Technical Secretariat practice to strictly control and protect even that “unclassified” information received from Member States. Furthermore, in accordance with Part VII of the OPOC, no information received from a Member State, regardless of classification, is available for public release unless the consent from that Member State has been obtained.

## **2. Authorised Representatives of Member States to the OPCW**

- 2.1 Paragraph 3.5 of Part VI of the OPOC requires that “*information, including that designated as confidential, which is passed to the Organisation by a State Party must be provided by an official representative of that State Party*”. In accordance with this requirement, staff of the Technical Secretariat are not authorised to transfer or receive confidential materials to/from representatives of Member States other than those designated as official representatives.
- 2.2 Permanent Representatives, Alternates and Advisers who, are accredited in accordance with the provisions of the respective Rules of Procedure of the Conference of the States Parties and the Executive Council, as well the relevant provisions of the OPCW Headquarters Agreement, as described in the Technical Secretariat’s document “(Permanent) Representatives, Alternates and Advisers accreditation”, S/112/99, dated 6 May 1999, are official representatives of Member States. In general, only Permanent Representatives and Alternates of Member States are entitled to receive confidential documents and materials from the Technical Secretariat.
- 2.3 Officials other than Permanent Representatives and Alternates may collect confidential documents from the Technical Secretariat on the authorisation of the relevant Permanent Representative to OPCW. This authorisation must be provided in advance, through an official letter or note verbale to the administrative unit of the Technical Secretariat that provided the notification that a document is ready for collection.

## **3. Marking of Confidential Documents**

- 3.1 When submitting or receiving confidential OPCW documents it is necessary that both the document and any external packaging in which it is enclosed be marked with proper OPCW classification markings in accordance with Part VI of the OPOC.

- 3.2 Confidential documents intended for circulation during a confidential session of one of the Policy-Making Organs of the OPCW, or one of their subsidiary bodies, must also be marked with proper OPCW classification markings and should be submitted to Declarations Branch (DEB) well in advance of the meeting at which they are to be circulated.

#### 4. Verification-Related Documents

- 4.1 The administrative unit of the Technical Secretariat tasked to receive and distribute verification-related documents is DEB.
- 4.2 **Delivery to the Technical Secretariat.** To deliver a confidential document to the Technical Secretariat, an authorised representative of the Member State should first make an appointment with DEB (telephone: 070-4163031). At the pre-arranged meeting time, delivery of the document by an accredited representative of the State Party shall be carried out in room B.12 of the OPCW Headquarters building in the presence of two DEB staff members. The two DEB staff members will verify the authorisation of the representative by means of his/her OPCW identity card.
- 4.3 The transfer of confidential material to the Technical Secretariat via e-mail, mail, courier or non-secure fax is not consistent with the provisions of the OPOC. Such means of transfer generally do not ensure the necessary level of protection required for OPCW confidential information. In cases where confidential material is received via one of these means, the Technical Secretariat shall handle that material, from the time it is received or opened, according to its internal procedures for handling and protecting confidential information. However, the Technical Secretariat can not guarantee that information provided in such a manner has remained free of unauthorised disclosure before its arrival. Member States are therefore asked, as a general rule, not to transfer classified information to the Technical Secretariat via e-mail, mail, courier or fax.
- 4.4 **Acknowledgement of documents.** The receipt of confidential documents and/or materials delivered directly to the Technical Secretariat by a Member State representative shall be acknowledged by a signed Confidential Material Consignment Note (form C16).
- 4.5 **Collection of confidential documents.** DEB shall notify the Permanent Representative of the Member State to the OPCW by fax that “a document” (without further specification if the title of the document is also confidential) is available for collection. In response to the fax Member States should contact DEB for an appointment to collect the confidential document (telephone: 070-4163031). At the pre-arranged meeting time, the document will be transferred to an accredited representative of the State Party in room B.12 in the presence of two DEB staff members. The transfer of the document(s) for which the notification is sent will be accomplished in accordance with all applicable confidentiality procedures. Should a member of a delegation, other than the Representative or an Alternate be required to collect the document, a

corresponding authorisation letter or note verbale issued by the Representative (as outlined in paragraph 2.3) must first be received by the Technical Secretariat. The two DEB staff members will verify the authorisation by means of the representative's OPCW identity card.

## **5. Distribution of Confidential Official-Series Documents**

5.1 Confidential official-series documents used for consideration in the meetings of the Policy-Making Organs of the OPCW are distributed by the Secretariat for the Policy-Making Organs.

5.2 The Secretariat for the Policy-Making Organs (PMO) will notify delegations via fax as to the availability of such documents using an unclassified title, and will designate two different time periods for collection of the document(s) by delegations. These times will be arranged on two different days to facilitate collection of the document(s) by all intended recipients. Only one copy of a confidential document will be distributed per Member State, to be collected by any one of its authorised recipients. Staff of the Technical Secretariat are not authorised to make copies of confidential documents collected by authorised representatives of Member States.

5.3 Staff of the Technical Secretariat are authorised to transfer confidential official-series documents only to duly authorised persons as described in paragraphs 2.2 and 2.3.

5.4 As required, PMO will contact those delegations that did not collect their copy of the confidential document(s) during the two prearranged time periods, and advise of a third and final date for collection.

## **6. Confidential documents other than Verification Related and Official Series Documents**

6.1 In the event of the need to transfer a confidential document (s) to/from any unit of the Technical Secretariat other than DEB/PMO, the same procedures for the handling and receipt of such documents shall be followed.

6.2 Questions related to any of the procedures outlined in this document may be directed to the Office of Confidentiality and Security (telephone: 070-4163366) or any of these specific administrative units of the Technical Secretariat mentioned in paragraphs above.

## Annex 1 - Classification categories (Excerpted from Part V of the OPCW Policy on Confidentiality)

OPCW RESTRICTED	OPCW PROTECTED	OPCW HIGHLY PROTECTED
<p><b>CRITERION:</b> This category comprises information of which the unauthorised disclosure would be prejudicial to the effectiveness or credibility of the Convention, or prejudicial to the interests of a State Party or of a commercial or governmental body or of a national of a State Party (para 1.7).</p> <p><b>EXAMPLES:</b> Unless specified otherwise, due to the greater or lesser sensitivity of the data in question, the following forms of information might be classified <b>OPCW RESTRICTED</b> when they are acquired or generated by any means by the Organisation (para 1.8):</p> <p>(a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by originating States Parties as being of this level of sensitivity;</p>	<p><b>CRITERION:</b> This category comprises information of which the unauthorised disclosure may cause substantial damage to the effectiveness or credibility of the Convention, or to the interests of a State Party or of a commercial or governmental body or of a national of a State Party (para 1.11).</p> <p><b>EXAMPLES:</b> Unless specified otherwise in accordance with greater or lesser sensitivity, the following forms of information might be classified as <b>OPCW PROTECTED</b> when they are acquired or generated by any means by the Organisation (para 1.12):</p> <p>(a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by the originating States Parties as being of this level of sensitivity;</p>	<p><b>CRITERION:</b> This category comprises sensitive confidential information of which the unauthorised disclosure would cause serious damage to the effectiveness or credibility of the Convention, or its aims and purpose, or cause serious damage from the point of view of national security or commercial secrecy to the interests of a State Party or of a commercial or governmental body or national of a State Party (para 1.14).</p> <p><b>EXAMPLES:</b> Unless specified otherwise in accordance with lesser sensitivity, the following forms of information might be classified as <b>OPCW HIGHLY PROTECTED</b> when they are acquired or generated by any means by the Organisation (para 1.15):</p> <p>(a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by originating States Parties as being of this level of sensitivity;</p>

OPCW RESTRICTED	OPCW PROTECTED	OPCW HIGHLY PROTECTED
<p>(b) general reports on the results and effectiveness of verification activities; and</p> <p>(c) information to be supplied to all States Parties in accordance with other provisions of the Convention.</p> <p>Other information to be classified and handled as <b>OPCW RESTRICTED</b> may include: routine confidential correspondence between States Parties and the Secretariat, and internal working documents of the Organisation which are not of particular sensitivity. This may also include information relating to the internal processes and decision-making of the Secretariat, and other managerial or administrative information, where open disclosure of the information might hamper the Organisation's effectiveness in implementing the Convention (para 1.9).</p>	<p>(b) unpublished technological information about production processes and facilities, and technical information about industrial products;</p> <p>(c) less sensitive or more general information related to commercial transactions and the cost factors of industrial processes and production;</p> <p>(d) detailed initial reporting on an inspection, including information on anomalies or incidents at facilities, and inspection reports;</p> <p>(e) data and information regarding inspection planning of the Secretariat and the inspection goals for a specific facility;</p> <p>(f) facility agreements and any attachments thereto; and</p> <p>(g) information regarding the validation and evaluation of information contained in declarations, facility agreements and inspection reports.</p>	<p>(b) samples taken from inspected sites and returned samples from designated laboratories, and results from analysis of samples;</p> <p>(c) especially sensitive confidential information especially provided by a State Party; and</p> <p>(d) confidential information for which access is normally only required, or voluntarily or incidentally provided, during the actual conduct of an on-site inspection, such as :  - process flow diagrams;  - photographs, plans and diagrams of the site;  - specific data related to technological processes and their parameters;  - analytical data of samples taken on site and analysed on site;  - commercially sensitive market</p>

<b>OPCW RESTRICTED</b>	<b>OPCW PROTECTED</b>	<b>OPCW HIGHLY PROTECTED</b>
	<p>Where such information is not considered relevant to verification of compliance, it will normally be treated initially as <b>OPCW HIGHLY PROTECTED</b>, even before any formal classification is determined, as specified in subparagraph 1.17 of this Part.</p>	<p>information, such as a detailed list of customers, and individual quantities sold to them; and</p> <ul style="list-style-type: none"> <li>- other detailed, highly specific technical, commercial or national security information.</li> </ul> <p>Where such information is not considered relevant to the verification of compliance, it will normally be treated initially as <b>OPCW HIGHLY PROTECTED</b>, even before any formal classification is determined, as specified in subparagraph 1.17 below.</p>
		<p>In most inspection scenarios, the highly sensitive information specified in subparagraph 1.15(d) above, that may or may not have a national confidential classification, may be kept at the inspected facility and shall only be made available for on-site use during the inspection. When such information is not taken off site and access to it is limited, there will accordingly be no application of the OPCW classification process within the Secretariat. Even so, during inspection activities the inspection team will give this</p>



<b>OPCW RESTRICTED</b>	<b>OPCW PROTECTED</b>	<b>OPCW HIGHLY PROTECTED</b>
		<p>information at least the level of protection afforded to information as <b>OPCW HIGHLY PROTECTED</b>. The classification category of such information should be specified to the extent possible in facility agreements (para 1.16).</p> <p>Sensitive confidential information not related to the verification of compliance which is incidentally revealed or collected by any member of an inspection team shall not be recorded in any form, and shall not be further disseminated. When access is afforded to such sensitive information during inspection activities, any member of the inspection team must give it at least the level of protection afforded to information classified as <b>OPCW HIGHLY PROTECTED</b>, until or unless the inspected State Party specifies particular handling or level of sensitivity. In such a case the inspected State Party may designate (as provided in subparagraph 2.5 of this Part) an initial classification of such information during the inspection process or in a facility agreement. In the event that such sensitive information is taken to the Secretariat inadvertently or by agreement with the inspected State Party, it shall be classified as</p>

<b>OPCW RESTRICTED</b>	<b>OPCW PROTECTED</b>	<b>OPCW HIGHLY PROTECTED</b>
<p><b>DISSEMINATION:</b></p> <p><b>OPCW RESTRICTED</b> information that must be routinely provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex shall be disseminated accordingly (para 1.10).</p>	<p><b>DISSEMINATION:</b></p> <p><b>OPCW PROTECTED</b> information that must be routinely provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex shall be disseminated accordingly (para 1.13).</p>	<p><b>OPCW HIGHLY PROTECTED</b>, and protected accordingly, unless the inspected State Party specifies otherwise (para 1.17).</p> <p><b>DISSEMINATION:</b></p> <p><b>OPCW HIGHLY PROTECTED</b> information that must be routinely provided to States Parties in accordance with subparagraph 2(b) of the Confidentiality Annex shall be disseminated accordingly (para 1.18).</p>