World Meteorological Organization **19.I.2017**

Summary of recommended from CBS-16 on amendment to: Manual on WIS, Guide to WIS and its attachments, Manual on GTS

CBS-16 recommended to Executive Council that Executive Council:

Confirms that, following confirmation by CBS-16 of technical compliance, the asterisk that denotes conditional designation in Table 2 of Appendix B to WMO-No. 1060 *Manual on the WMO Information System* can be removed from those WIS Data Collection or Production Centres (DCPCs) listed in Table 1 of Annex 1;

Endorses the proposal from CBS-16 that updating the value assigned to "WMO_DataLicenseCode" in the WIS discovery metadata record describing shared information should be the mechanism used by Permanent Representatives to notify the Secretary-General, Members and third parties of the data policy to be applied to that information, and that a letter from the Permanent Representative should no longer be required;

Decides in respect of WMO-No. 1060 *Manual on the WMO Information System* and WMO-No. 1061 *Guide to the WMO Information System* to:

(1) Designate as WIS DCPCs those centres listed in Table 2 of Annex 1 and add them to Table 2 of Appendix B to WMO-No. 1060 *Manual on the WMO Information System*;

(2) Update the country name for NMC (Aruba) to Aruba (Netherlands) in Table 3 of Appendix B to WMO-No. 1060 *Manual on the WMO Information System*;

(3) Update the principal GISC for NMC Algeria, RTH/RSMC-Geographical (Algiers) and NMC Tunisia to be Toulouse and record this in Table 3 of Appendix B to WMO-No. 1060 *Manual on the WMO Information System*;

(4) Editorially correct the name in French of the Radar Data Centre in Toulouse in the French version of Table 2 of Appendix B to WMO-No. 1060 *Manual on the WMO Information System* to "Centre de données radar OPERA";

(5) Amend the text of WMO-No. 1060 *Manual on the WMO Information System* and WMO-No. 1061 *Guide to the WMO Information System* in respect of the WMO Core Metadata Profile as in Annex 2;

(6) Add new Part VI "Information Management" is to the Manual on the WMO Information System (WMO-No. 1060) and Part VII with the same title to the Guide to the WMO Information System (WMO-No. 1061) and introduce the text in Annex 3;

(7) Pending development of provisions relating to information management, the text of Part VI of the Manual on the WMO Information System (WMO No. 1060) should be: "Note: guidance on information management best practices is provided in Part VII of the Guide to the WMO Information System (WMO No. 1061)";

(8) The contents of Annex 3 on Information Management should be published as Part VII of the Guide to the WMO Information System (WMO No. 1061);

(9) Designate the text in Annex 4 on DBNet as Technical Specifications (to allow amendment using the fast-track (simple) procedure) and publish it as a document with its own WMO publication number as an Attachment to WMO-No. 1061 *Guide to the WMO Information System*;

Further decides in respect of WMO-No. 386 *Manual on the Global Telecommunications System* and its associated guidance documents to**:**

(1) Update the requirements for World Weather Watch quantitative monitoring to reflect advances in technology and the introduction of WIGOS as specified in the amendments to WMO-No. 386 *Manual on the Global Telecommunications System* specified in Annex 5 to the present Resolution;

(2) Amend WMO-No. 386 *Manual on the Global Telecommunications System* Part 1 and Attachments I-2 and I-3 as specified in Annex 5 to reflect the current structure of the Global Telecommunications System (GTS) and to record information on the structure of the GTS that is still required and that was previously recorded in Volume II of that Manual;

(3) Amend as specified in Annex 6 the recommended practices for the use of the TCP/IP protocol on the GTS that are recorded in Attachment II-15 of WMO-No. 386 *Manual on the Global Telecommunications System*;

(4) Amend as specified in Annex 7 WMO-No. 1115 *Guide to Information Technology Security* to reflect modern practices;

(5) Amend as specified in Annex 8 WMO-No. 1116 *Guide to Virtual Private Networks (VPN) via the Internet between GTS centres* to reflect modern practice;

_____

Annex 1
Amendments to WMO-No. 1060 Manual on WMO Information System recommended by CBS-16

Amendments in Recommendation 3.4(1)/1 (CBS-16) – *Updates to the Manual on the WMO Information System*

Table 1 – Approval of WIS Data Collection or Production Centres conditionally designated under Resolution 51 (Cg-XVI)

Remove the asterisk (*) denoting conditional designation from Table 2 of Appendix B of WMO No. 1060 Manual on the WMO Information System *to "Centre de données radar OPERA"*

WMO Member or Contributing Organization	Name	Centre location region / city		Principal GISC	Const. Body
India	RSMC-Activity-TC	II	New Delhi	New Delhi	CBS
Netherlands	RCC–De Bilt	RA VI	De Bilt	Exeter	CCl
Norway	Norwegian Institute for Air Research (NILU)	RA VI	Kjeller	Offenbach	CAS

Table 2 – Proposed additions to Appendix B, Manual on WIS list of WIS Data Collection or Production Centre

Add the following entries to Table 2 of Appendix B of WMO No. 1060 Manual on the WMO Information System *to "Centre de données radar OPERA"*

WMO Member or Contributing Organization	Name / Function	Centre location region / city		Principal GISC	Const. Body
Argentina	VAAC	III	Buenos Aires	Brasilia	CAeM
	RTH	III	Buenos Aires	Brasilia	CBS
	RSMC-Geographical	III	Buenos Aires	Brasilia	CBS

Amend the following entries in Table 3 of Appendix B of WMO No. 1060 Manual on the WMO Information System *[this Table is not in the CBS document – the amendment implements the **decides(3)** text]*

WMO Member or contributing organization	Centre name	GTS function	Centre Region location		Principal GISC	Constituent body
Algeria	Office National de la Météorologie	NMC	I	Algiers	~~Casablanca~~ Toulouse	CBS
~~Netherlands~~ Aruba (Netherlands)	Departamento Meteorologico Aruba	NMC (Aruba)	I V	Aruba	Washington	CBS

_____

Annex 2

[This text is copied from the Annex to Recommendation 3.4(2)/1 (CBS-16)]

TEXT FOR INCLUSION IN THE MANUAL AND GUIDE TO THE WMO INFORMATION SYSTEM

Amend paragraph 5.4 of Part V "WIS Discovery metadata" of the Manual on WIS (WMO-No. 1060)

5.4 **CBS shall maintain and develop the WMO Core Metadata Profile. ~~Changes to the WMO Core Metadata Profile shall be governed using the procedures defined in Appendix C to this Manual.~~**

Note: Resolution 12 (EC-68) designated Appendix C Part 2 section 3 (Data Dictionary) as technical specifications for the purposes of managing amendments.

Note: Guidance on application of the WIS Core Metadata Profile is available in Part V of the *Guide to the WMO Information System* (WMO-No. 1061).

Amend the first paragraph in section 9.3 of Appendix C Part 1 of the Manual on WIS (WMO-No. 1060)

WMO data policy pertaining to Resolution 40 (Cg-XII), ~~and~~ Resolution 25 (Cg-XIII), Resolution 60 (Cg-17) or ~~and~~ other regulations (e.g. ICAO Annex 3 – Meteorological Services for International Air Navigation) shall be expressed using the following controlled vocabulary: "WMOEssential", "WMOAdditional" and "WMOOther".

Note: Inclusion of the data policy in a metadata record describing information satisfies the requirements in the above resolutions to notify the Secretary-General or third parties of limitations on the use of the information described in the metadata record (Resolution XX, EC-69). Additional information on the type of restriction on use should be included in the metadata record if the text in the Resolution does not describe the restriction adequately. Further information on describing data policy is provided in the *Guide to the WMO Information System* (WMO-No. 1061).

Add the text of the Annex to Resolution 12 (EC-68) to the Guide to the WIS WMO-No. 1061 .

Add the following as the first paragraph in Part V "Metadata Guidance" of the Guide to the WIS (WMO-No. 1061)

Note: Resolution 12 (EC-68) designated Part V section 3 (Metadata Guidance) as technical specifications for the purposes of managing amendments.

Replace the original text in Part V "Metadata Guidance" of the Guide to the WIS (WMO-No. 1061) with the following text.

Guidance for creating WMO Core Profile Metadata in version 1.3

Introduction

Metadata records, by providing the product information that will allow WIS users to discover access and retrieve products, have a very important role in the WMO Information System (WIS). Metadata has to adhere to standards (such as standard vocabularies, and standard schemas) to ensure product definition homogeneity, and to contribute to making systems interoperable. There are a number of metadata standards that address the needs of meteorological and hydrological communities. The WIS "discovery" metadata standard (for

dataset discovery catalogues), is called the "WMO Core Profile 1.3". It is a profile of the ISO 19115:2003 metadata standard, with its associated ISO 19139 XML mapping. ISO19115 is a complex standard, and the creation of high quality ISO19115 metadata records can require both organizational expertise and subject expertise, in order to describe an object, and its context for use.

This guidance documentation is intended for metadata authors or product/infrastructure specialist who would like to create WMO Core Profile 1.3 (WMCP) metadata records for making their datasets discoverable within the WMO Information System (WIS) catalogue(s). It will also assist those who wish to create high quality WIS metadata records for data that will be ingested and distributed by a WMO GISC.

This Guidance documentation suite is composed of the present document, and associated WMO Core Profile Templates (see Section 0 References) which can be used to create individual metadata records, or to automate the creation of several records. It also provides a set of recommendations to be followed, in order to provide the right level / granularity of product information in the WMO Core Profile metadata records.

References

WMOCore Profile 1.3 Template XML records:

Template records containing PLACEHOLDERS (to be replaced with content) are available from

http://wis.wmo.int/MD-Templates

A valid example XML record, containing example field content (to be replaced) is also available there.

WMO WIS Wiki Page:

http://wis.wmo.int/MD_Index

WMO Core Profile documentation:

Part 1: http://wis.wmo.int/WCMPpart1
Part 2: http://wis.wmo.int/WCMPPart2

This GUIDANCE WMO Core Profile documentation suite:

http://wis.wmo.int/MD_Index or http://wis.wmo.int/WIS-Manual (for a summary of changes)

Additional WMCP Metadata Examples (for particular product types):

http://wis.wmo.int/MD-Examples

WIS Discovery Metadata

WMO Core Profile Presentation

The WMO Core Profile (WMCP) v1.3, while sometimes referred to as "discovery" metadata, is also aimed at providing catalogue users with sufficient information for them to decide on the suitability of the data, and to provide access to, or details on how to access the data. Some of the information contained in a WMCP metadata record is vital for optimizing the searching functionality offered by the WIS Product catalogues. In the WIS, users typically need to search one of the WIS catalogues, for discovering and accessing products.

A "discovery" metadata record has to contain the following components of information, to help users understand that product: What, When, Where, Who, How. A summary overview is provided below, and details are provided in Section 9.1.

(a) Product Information:

- **What**: This is the product content, and it is mainly defined by the Product Title and the Product Abstract fields, though additional fields can also be used. The information in the title and abstract is very important because the Product Title and Abstract are indexed by any Product catalogue, and thus searchable. In addition, the title and part of the abstract are presented to users, in the search results of each WIS Catalogue, and so good content here can assist users' efficiency in their "search, view search results, and decide" activity.

- **When**: This is the temporal coverage of the dataset or product, and is captured in the "temporal extent" section of the metadata record. It is possible to describe on-going, finite, or 'rolling window' datasets.

- **Where**: This is the geospatial extent of the dataset, describing which geographical area(s) the product covers, over the Earth or atmosphere. It can be the full Earth, a region or a specific place. In the WMCP, if the data is geographical, the metadata record must define as at least one bounding box with latitude-longitude coordinates, but that information can also be enhanced by using geographical identifiers for geographical regions, features (such as coastlines) and the like.

- **Who**: This is the contact details of the organization that is responsible for the product; the contact details of the organization responsible for the metadata, and (optionally) the name of the party that should be "cited", when referencing the data. It's possible, but not necessary for the same party to be responsible for both the metadata and data.

- **How - Data access and use**: This information is composed of the distribution information, but also includes the data policy, or terms and conditions for accessing the product. Most of the time, the distribution section offers a URL linking to a data access service. The data access service might require registration, and /or might offer sub-select/sub-sampling of the product. Currently, users wishing to access information that has the Data Policy (shown in "ResourceConstraints") of “WMOAdditional” must be registered with their regional GISC. Data with a Data Policy of "WMOEssential" can be accessed

wihout restriction. Users wishing to set up a “subscription” service, however, must register, regardless of the type of information they require.

(b) **WIS necessary technical information**: Section 9.2 of this document defines the set of information required, to have a functioning, distributed WIS infrastructure. This includes, for instance, the WIS unique identifier for each metadata records.

WMO Core Profile and ISO standard

The WMO Core Profile 1.3 is a customization, also called a profile, of the more generic ISO 19115 discovery metadata standard. It allows the meteorological community to better define meteorological products (terrestrial, Earth observations, numerical weather predictions model outputs). The ISO 19115 structure is detailed and complex, because it was designed to accommodate a wide range of information resource types. The WMO Core Profile, as well as providing more targeted searching, aimed to remove the need to understand some of those intricacies of ISO19115. This Guide aims to simplify the knowledge needed by users who are starting to create WMO Core Profile v.1.3 metadata records.

WMO Core Profile Metadata Granularity and Scope

One difficulty, when creating a metadata record, is to understand what level of detail of a dataset should be described, in the record for a particular product/dataset. Some products of the same type are continuously produced, during the life time of a satellite, or as model forecast outputs. Creating a new metadata record for each individual satellite instrument measurement granule (produced every three minutes), or for each forecast run (produced three times a day) would make the WIS catalogues' content grow at a huge rate, and the thousands of new metadata records would contain the same information, apart from the measurement time. This would dramatically damage the catalogue search experience, and would make it difficult to find products.

To solve that problem, the creation of one metadata record for an entire “collection” of "like" products is generally recommended, provided that effective searching, and other WIS infrastructure needs are not compromised. An example of "like" products is where each observation product only varies within one or two dimensions (time, geographical position, etc.), while still coming from the same measurement instrument or station. An example of this approach is the EUMETSAT Meteosat Second Generation (MSG) Seviri Level 1.5 dataset which includes all the level 1.5 radiances over the entire MSG mission with a global coverage, and is described by one unique metadata record. The user discovering this product collection, via the WIS portals, is re-directed to a EUMETSAT service offering sub-sampling capacities for selecting the interesting time period and geographic region.

That said, it is up to the data provider to decide what is a valid collection. To assist, IPET-MDRD has defined, in the Annex Section 12 (**Collection Definition Criteria**), a set of “granularity” criteria to consider when defining a collection metadata record.

WIS product Categories

Two forms of information (and corresponding transport protocols) are used in WIS catalogues:

(a) **GTS-delivered data**. This is mainly, but not exclusively, traditional WMO 'bulletins';

(b) **Non-GTS-delivered data**. This can include both data stored as files, and data as services.

(a) The first category is governed by the set of regulations described in the *Manual on the GTS* (WMO-No. 386), including the bulletin header (abbreviated header line) which identifies a bulletin like ISMS01 AMMC.

Metadata records for GTS bulletin datasets need to follow a set of additional rules, and require an understanding of the GTS regulations. Non-bulletin files can also be distributed via the GTS.
The most notable feature is the store-and-forward delivery mechanism for bulletins and other data on the GTS. This is the reason that there used to be no URL for a bulletin - once a bulletin is delivered, it is not retained for later reference.

Today, GISCs serve bulletins issued in the past 24 hours, but the common practice is still that a metadata record for bulletins does not include the access URL(s).

(b) The second category includes datasets described and searchable from the WIS catalogues, but which are served from the different responsible organizations, via their own infrastructure and data access services. WMO Core Profile (WMCP) 1.3 metadata records for this second category have to follow a minimum set of rules, to stay compliant with the standard. This is a subset of the rules which apply to GTS-served data.

Typically, these metadata records include a URL for access to the data.

This guide provides extensive support for creating the different information parts of a metadata record, for both non-GTS and GTS delivered datasets. When necessary, an additional section for creating metadata records for GTS bulletins has been added, in each information category (e.g. Product information abstract).

COMPLIANCE to additional metadata standards

This guide provides information to help create metadata records that comply with WMO Core Metadata Profile (**WMCP**) v.1.3. The WMCP Profile is based on ISO-19115 (Geographic information — Metadata standard). ISO 19115 provides two profiling mechanisms:

(i) Recommending a more constrained use of ISO19115 (either by recommending use of less fields, making an optional element mandatory, or constraining the expected content of a field) - to suit the needs of a particular community; and

(ii) In addition to (i), defining additional non-ISO19115 fields (and field content) to be added to any record.

Examples of type (i) ISO19115 profiles, in addition to the WMCP, include the INSPIRE Metadata Profile (Infrastructure for Spatial Information in the European Community), the North American Profile, the Australian and New Zealand Metadata Profile (ANZLIC) and UK GEMINI.

An example of (ii) is the Marine Community Profile. For more information see also http://www.dcc.ac.uk/resources/metadata-standards/iso-19115.

Each ISO19115 profile defines specific rules that should be met. For example, to comply with the INSPIRE metadata profile, the additional requirements to be met include the provision of one keyword from the general environmental multilingual thesaurus (GEMET), a lineage statement and a conformance statement to Regulation (EC) No. 1205/2008.

The content of a WMO Core Profile 1.3 metadata record, defined following this current guide, can be extended, so that the record also supports additional profiles (such as, for instance, INSPIRE or ANZLIC). In such a case, the metadata author is required to implement any additional requirements specified in the corresponding profile's documentation. The extended WMO Core Profile 1.3 metadata record can still be published on the WIS.

WMO Core Profile - Validation Tools

Metadata publishers are required to ensure that created metadata records conform to relevant technical specifications. For example, XML documents need to be well-formed, schema-valid, and conformant with other requirements imposed by the specifications.

A set of ISO and WMCP validation tools can be used, to ensure that a created WMO Core Profile record is correctly formatted (syntactically and semantically), and can be ingested by a GISC.

In most cases, to validate metadata, the metadata author will need a local copy of the metadata record, or the URL of the metadata file, and offer the local location or URL in an online service, or with a locally installed validation software. Online validation services can automatically evaluate the content of the metadata in terms of the completeness, accuracy and conformance. Some validation tools, such as the one developed by NOAA (http://www.ngdc.noaa.gov/docucomp/recordServices) may give a score based on different aspects including content and quality of metadata.

It is recommended to test the metadata with one of the available tools. It is also always possible to seek assistance from your Principal GISC.

Below is a list of web services and tools used to validate WMO Core Profile 1.3 and ISO 19115/19139 metadata records.

WMO Core Profile 1.3 validation services/tools:

- **NOAA's WMO validation service**: http://www.ngdc.noaa.gov/docucomp/validationServicesWmo
- **GeoNetwork-ANZMEST, with WMO Core Profile Validation**
- https://sourceforge.net/projects/anzmest/files/bom-releases/
  This directory has the Bureau of Meteorology releases of ANZMEST 2.10.x (based on GeoNetwork), which includes WMO Core Profile 1.3 editing and validation tool.
  For instructions on running the software and validation, see the WIS Wiki page on validation tools [below]

WIS Wiki page on validation tools : http://wis.wmo.int/MD-Validate

ISO 19115/19139 validation services/tools:

- NOAA ISO validation page: http://www.ngdc.noaa.gov/docucomp/recordServices
- GeoNetwork-ANZMEST – BOM branch
- https://sourceforge.net/projects/anzmest/files/bom-releases/ (includes 19115:2006, 19115:INSPIRE)

Principles of metadata management on the WIS

The Global Information System Centres (GISCs) are responsible for the management of metadata. According to the WMO technical regulations, each GISC shall:

- Provide a comprehensive metadata catalogue with discovery services for all National Centres (NC) and Data Collection and Production Centres (DCPC) data content across the WIS,
- Support the Search and Retrieve via URL protocol (SRU),
- Ensure the synchronization of metadata among GISCs, using the OAI-PMH protocol,
- Support user's identification and authorization, including in terms of metadata maintenance,
- Provide metadata publishing facilities: Using Uploading/Harvesting metadata publishing or on-line Metadata editing to allow Metadata author creating metadata records.

How to publish metadata?

- Metadata could be published at DCPC or GISC level,
- Find which GISC you belong to (i.e. which is your principal GISC). The official reference of WIS centres (GISCs and affiliated DCPCs and NCs, areas of responsibility) is the Annex VII to the WMO Technical Regulations, *Manual on WIS* (WMO-No. 1060), ***Annex B Approved WIS Centres***. The list of GISCs, and related links, is also available online on WMO portal: https://www.wmo.int/pages/prog/www/WIS/centres/index_en.php. The procedure to be used for metadata management (account creation, editing facilities, ...) may vary between centres, but will usually be via the GISC portal (at least, as a first point of contact),
- Proceed to registering on your principal GISC (this could be done online, depending on GISC's capabilities or policies), after which you will be assigned a username and a role,

- Publish your metadata via your principal GISC: In order to publish your metadata records, use the appropriate method among those allowed by the GISC (import/insert metadata, or harvest metadata using OAI-PMH). Note: For a limited number of records, it is typically also possible to use a GISC's online editing services.

For more comprehensive information regarding the WIS and publishing metadata on the WIS, please consult the WIS Manual (http://wis.wmo.int/WIS-Manual).

Generating WMO Core Profile METADATA

This guide is intended to help product specialists create WIS metadata records which are compliant with the WMO Core Profile 1.3. It provides practical guidance on key information needed in WMCP metadata creation (such as describing how, and where, to insert the necessary product information into a template record, and the WIS specific information required in the XML metadata record), while abstracting (as much as possible) the WMO Core Profile standard, the ISO 19115 standard and its XML mapping (ISO 19139).

The current guide defines [in Section 9: "Necessary Information to create a WMO Core Profile "] a set of recommendations for adding each individual piece of information regarding a product (title, abstract, data responsible party, data access, etc.).

This guide uses an **XML template** based approach. A metadata author consulting this guide should use a copy of the **Template xml record**(s) [the url to access these is indicated in the "References" section of this document) in conjunction with this Guide, especially Section 9. "Necessary Information to create a WMO Core Profile ".

The template-based approach allows a person without any knowledge of ISO 19115 to create an XML WMO Core Profile metadata record populated with the key information needed to make the record easily searchable and accessible within a WIS portal.

The template files can also be used as the foundation for building a web-based editing tool where the user completes a web form, and the content is used to overwrite the placeholders, and create the final WMO Core Profile 1.3 compliant metadata record.

Template-based principle

The Template xml files are metadata records encoded as xml. These contain PLACEHOLDERS, that is: GENERIC-TEXT that should be replaced with information related to the specific product that the WIS discovery metadata record describes.

Placeholders in the 2 template files are all in capital letters, in the form of, for instance:

```
ADD-CREATION-DATE*M or PRODUCT-TITLE*M.        i.e.    <xml field name>ADD-
                    ORGANISATION-NAME*M</xml field name>
```

The 2 **Template** WMCP xml metadata records are "WMCPv1.3 _MAND-**Template**.xml" and "WMCPv1.3 _OPTandMAND-**Template**.xml" (see Section 0: References, for its access url).

There is also a "WMPv1.3 _OPTandMAND-**Content**.xml" file, which has example content, rather than the placeholders. This latter is a valid WMCP record, which can be added into any editor, and then modified, or can be manually edited.

As well as PLACEHOLDERS, the two Template files contain hints and comments, formatted as follows:

```
<!--  this is a comment : use this XML block, if …..., otherwise, remove it    -->
```

Metadata content discussed in this Guidance document (and for which there are placeholders) includes all mandatory WMCP content, and some key content that is optional. The optional elements can be one of the following:

(i) Highly recommended [*HR]

(ii) Conditionally mandatory [*C]

(iii) Likely to be needed [*O]
*(As noted elsewhere, other ISO19115 elements, while not mentioned in the WMCP v1.3 documentation, may also be deemed useful, and **can** be used within a WMCP record. An example might be the DataQuality section, or the SupplementalInformation field. For reasons of brevity, however, these have been omitted from this document.)*

An example of (iii) is Section 9.1.7 Geographic Identifier.

An example of (ii) is Section 9.1.6 Geographic Bounding Box (which is only mandatory if the dataset is geospatial) or Section 9.1.10 Data Policy, which, while OPTIONAL, is mandatory if the product is GTS data.

An example of (i) is Section 9.1.5 Product Temporal Information, which, while OPTIONAL, is highly recommended.

Note that many optional <<subsections>> of a WMCP record contain elements which are mandatory **only if** that subsection is used. These are marked with "-MW", meaning "mandatory within subsection".

An example of that is the .. 'identifier'/'authority'/'title', as shown on lines 53-57, in the ANNEX's hierarchical list of fields (and in excerpt below), where 'identifier' is optional ([0..n]), and even if it is used, 'authority' is optional ([0..n]); however, if 'authority' **is** used, then 'title' is mandatory ([1..1]).

```
53 _ ._ ._ ._ ._ .identifier_ ._ .ISO[0..n]
54_ ._ ._ ._ ._ ._ .MD_Identifier
55_ ._ ._ ._ ._ ._ ._ .authority_ ._ .ISO[0..1]
56_ ._ ._ ._ ._ ._ ._ ._ .CI_Citation
57_ ._ ._ ._ ._ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
```

(Excerpt from ANNEX, Section 13)

The cardinality notation of [x..y] indicates the minimum and maximum allowable times that the element may be used, within that part of the hierarchy/tree. For instance: [0..n] means that the element is optional, but can also be used any number of times; the notation of [1..2] means that it is mandatory, and may be used a maximum of two times. Refer to the ANNEX

for a hierarchical list of the main elements mentioned in this document, and their cardinality. ***Placeholders for WMCP mandatory content end with *M.***

The "WMOCoreProfile1.3 _OPTandMAND-**Template**.xml" file contains placeholders for all mandatory and optional elements that have been mentioned in this Guidance document. The "WMOCoreProfile1.3 _MAND-**Template**.xml" file contains placeholders for all mandatory elements mentioned in this Guidance document.

Where the metadata author chooses not to populate an **optional** field, then ***the related xml block (as indicated in the comments in the 2 template files) should be removed.***

A metadata author can, by following placeholders in the Template file, and the guidance recommendations in Section 9: [" Necessary Information to create a WMO Core Profile "], replace the different PLACEHOLDERS, and follow the <!-- comments --> in the template file, to create a WMO Core Profile 1.3 compliant record.

The 2 template WMCP xml metadata records, with only the placeholders, can be used as a starting template record for automating the generation of metadata records.

Necessary Information to create a WMO Core Profile COMPLIANT METADATA Record

Section 9 describes the information components needed, to build a meaningful metadata record. For each individual component, it includes:

- ***TEMPLATE Value:*** the template XML record's placeholder value(s), which are to be replaced;
- A summary of the type of information (from the metadata creator) that should replace the placeholder;
- ***Necessity:*** whether the component is always mandatory, conditionally mandatory, highly recommended or is optional, within WMO Core Profile 1.3;
- ***XPath:*** its location within the WMCP XML metadata record; and
- Example XML for that component, containing example content, instead of the Placeholder(s).

The metadata creator should, while reading the documentation, open the relevant metadata template record, and find the corresponding placeholder(s), which are to be replaced by the relevant product information.

For each component, this Guidance document offers a description of what is generally required for a Product, followed, where relevant, by details of what is required in a WMCP record for GTS Bulletin-specific metadata.

Product Information

Product Title

9.1.1 Product Title	
TEMPLATE Value:	ADD-PRODUCT-TITLE*M, ADD-ALTERNATE-TITLE*O
Information:	Product Name
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	Product information
XPath:	/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:citation/*/gmd:title/*/text() (Line 45 in ANNEX, Section 13)

The Product Title and the Product Abstract are the two most relevant elements in the WCMP metadata record, in the context of the WIS Product catalogues, as those two elements are presented to the users in the search results and product description page. They therefore need to focus on highlighting the product's key characteristics, to assist users searching for relevant products.

The title should be as specific about the product as is possible. If the product only contains one parameter, for instance, this can be stated in the title; however, if the product contains many parameters, then a more general term should be used in the title, and the parameters stated elsewhere in the metadata record (the abstract and/or the keywords). For a satellite product offering one main data parameter, the title will typically define which parameter is contained in the product, and from which instrument or instrument type it originates. For instance “AMSR-2 Sea Surface Temperature” or “SLSTR L1B radiances and brightness temperatures”.

Below is an example:

```
<gmd:identificationInfo>
   <gmd:MD_DataIdentification>
      <gmd:citation>
         <gmd:CI_Citation>
            <gmd:title>
               <gco:CharacterString>AMSR-2 Sea Surface Temperature</gco:CharacterString>
            </gmd:title>
            <gmd:alternateTitle>
               <gco:CharacterString>
               AMSR-2 Sea Surface Temperature SST
               </gco:CharacterString>
            </gmd:alternateTitle>
          . . . . . .
               </gmd:CI_Citation>
            </gmd:citation>
        . . .. .
   </gmd:MD_DataIdentification>
</gmd:identificationInfo>
```

- **Title for GTS bulletins**

The title for a GTS bulletin should also aim to be specific about the product, describing, as much as possible, the type of observation, and including the bulletin code or identifier, and original distributor (e.g. "from XXX").

For instance:

```
<gmd:identificationInfo>

    <gmd:MD_DataIdentification>

      <gmd:citation>

        <gmd:CI_Citation>

          <gmd:title>

            <gco:CharacterString>Sea level observations data [ SZPS01 ] for the South Pacific area.
CREX encoded. Every 3 minutes or as required (available from AMMC).</gco:CharacterString>

          </gmd:title> …
```

Product Abstract

9.1.2 Product Abstract	
TEMPLATE Value:	ADD-PRODUCT-ABSTRACT*M
Information:	Abstract describing the product
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:abstract/*/text()*

The product abstract is important in the context of the WIS catalogues, as it is part of the product information that is presented in the search results page. It should describe aspects which the data producer judges as important, and which will enable potential users to understand the key characteristics of, and nature of the product, so that they more quickly judge the suitability of that product for their needs.

The following structure of the abstract is recommended, in order to create a more coherent and homogenous set of data product descriptions, on the WIS. Having product abstracts structured similarly will help users who are comparing related and different data products.

The product abstract should complement the title by more accurately explaining the title's content, and should provide further detail, where appropriate, describing the product and in particular the source of the data (such as the instrument type or model when applicable), the coverage, production frequency (hourly, every 3 minutes, etc.), the data processing level (near real-time, derived, quality controlled), the available formats, and the data access services when relevant.

Below are typical abstracts for

(a) A NWP product:

Title: Copernicus Atmosphere Service MACC-IFS near real-time 5-day forecast of global black carbon aerosol concentration

Abstract: This service provides pre-operational daily forecasts up to 5 days of global black carbon aerosol using the IFS-LMD aerosol model. The product black carbon aerosol mixing ratios at 60 model levels. There are two forecasts per day, with base times of 00:00UTC (5-day forecast) and 12:00UTC (1-day forecast). Forecast steps are available at 3-hourly intervals and the spatial resolution is 0.75x0.75 degree. The forecast fields are generated in GRIB.

(b) A Satellite Observation Product

Title: IASI Atmospheric Temperature Water Vapour and Surface Skin Temperature - Metop

Abstract: The Atmospheric Temperature, Water Vapour and Surface Skin Temperature (TWT) product contains the vertical profiles of atmospheric temperature and humidity, with a vertical sampling at 101 pressure levels, and surface skin temperature. The vertical profiles are retrieved from the IASI sounder measurements (of IASI L1C product) together with collocated microwave measurements (AMSU & MHS 1B) when available. The main objective of the Infrared Atmospheric Sounding Interferometer (IASI) is to provide high-resolution atmospheric emission spectra to derive temperature and humidity profiles with high spectral and vertical resolution and accuracy. Additionally it is used for the determination of trace gases, as well as land and sea surface temperature, emissivity and cloud properties. The products are provided at the single IASI footprint resolution (which is about 12 km with a spatial sampling of about 25 km at Nadir). The quality and yield of the vertical profiles retrieved in cloudy IFOVs is strongly related to the cloud properties available in the IASI CLP product and the availability of collocated microwave measurements.

More examples for Metadata Titles and Abstracts can be found in the WIS Wiki http://wis.wmo.int/WIS-MD-Examples

Abstract for GTS bulletins

For the SMPS02 bulletin:

Title: SMPS02 SYNOP reports (pressure, wind and temperature) –South Pacific area; Available from NZKL (WELLINGTON/KELBURN) at 00, 06, 12 and 18 UTC

Abstract:

This bulletin dispatches synoptic data (pressure, temperature and wind) every 6 hours, starting at 0 UTC. The bulletin includes reports from the following stations: 91823 (NIUE AERO AWS) and 91962 (PITCAIRN ISLAND AWS).

Data Type: Surface data - Main synoptic hour - South Pacific area.

Actual data parameters sent include: Pressure, Pressure reduced to mean sea level, 3 hour pressure-change, characteristic of pressure change (increasing/decreasing), temperature (dry-bulb and dewpoint), wind direction, and wind speed.

Format: FM 12 (SYNOP, Report of surface observation from a fixed land station). (Refer to WMO No.306 - Manual on Codes for the definition of WMO international codes)

---- The SMPS02 TTAAii Data Designators decode (2) as:
T1 (S): Surface data.
T2 (M): Main synoptic hour.
A1A2 (PS): South Pacific area.
(2: Refer to WMO No.386 - Manual on the GTS - Attachment II.5)

Metadata Responsible Party

9.1.3 Metadata Responsible Party	
TEMPLATE Value:	ADD-METADATA-CONTACT-ORGANISATION-NAME*M; ADD-ADDRESS-STREET*O; ADD-CITY*O; ADD-REGION*O; ADD-POSTCODE*O; ADD-COUNTRY*O; ADD-EMAIL-ADDRESS*HR ; ADD-ORGANISATION-WEBSITE*O.
Information:	Responsible party for the created metadata record
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	Administrative information
XPath:	*/gmd:MD_Metadata/gmd:contact/gmd:CI_ResponsibleParty*

This element describes the contact details (address, telephone, email) of the party responsible for the metadata. For example:

```
<gmd:MD_Metadata>
   …... .. .. .
   <gmd:contact>
        <gmd:CI_ResponsibleParty>
            <gmd:organisationName>
                <gco:CharacterString>EUMETSAT</gco:CharacterString>
            </gmd:organisationName>
            <gmd:contactInfo>
                <gmd:CI_Contact>
                    <gmd:address>
                        <gmd:CI_Address>
                            <gmd:deliveryPoint>
                                <gco:CharacterString>EUMETSAT Allee 1</gco:CharacterString>
                            </gmd:deliveryPoint>
                            <gmd:city>
                                <gco:CharacterString>Darmstadt</gco:CharacterString>
                            </gmd:city>
                            <gmd:administrativeArea>
                                <gco:CharacterString>Hessen</gco:CharacterString>
                            </gmd:administrativeArea>
                            <gmd:postalCode>
                                <gco:CharacterString>64295</gco:CharacterString>
                            </gmd:postalCode>
```

```
                            <gmd:country>
                                <gco:CharacterString>Germany</gco:CharacterString>
                            </gmd:country>
                            <gmd:electronicMailAddress>
                                <gco:CharacterString>ops@eumetsat.int</gco:CharacterString>
                            </gmd:electronicMailAddress>
                        </gmd:CI_Address>
                    </gmd:address>
                    <gmd:onlineResource>
                        <gmd:CI_OnlineResource>
                            <gmd:linkage>
                                <gmd:URL>http://www.eumetsat.int</gmd:URL>
                            </gmd:linkage>
                        </gmd:CI_OnlineResource>
                    </gmd:onlineResource>
                </gmd:CI_Contact>
            </gmd:contactInfo>
            <gmd:role>
                <gmd:CI_RoleCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codelist/gmxCodelists.xml#MD_ScopeCode" codeListValue="pointOfContact">pointOfContact</gmd:CI_RoleCode>
            </gmd:role>
        </gmd:CI_ResponsibleParty>
    </gmd:contact>
```

Product Responsible Party

9.1.4 Product Responsible Party	
TEMPLATE Value:	ADD-PRODUCT-RESPONSIBLE-PARTY-ORGANISATION-SHORTNAME*M, ADD-PRODUCT-RESPONSIBLE-PARTY-EMAIL*HR
Information:	Organization responsible for the product described in the metadata record
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:pointOfContact/gmd:CI_ResponsibleParty*

This element contains the contact details of the organization responsible for the product. A minimum of a name and an e-mail address are required, and the role should be "pointOfContact".

```
<gmd:MD_Metadata>
   …... .. .. .
 <gmd:identificationInfo>
   <gmd:MD_DataIdentification>
```

```
      <gmd:citation>
       .. .. .. .. .
      </gmd:citation>
      .. . . . . . .
      <gmd:pointOfContact>
         <gmd:CI_ResponsibleParty>
            <gmd:organisationName>
                <gco:CharacterString>EUMETSAT</gco:CharacterString>
            </gmd:organisationName>
            <gmd:contactInfo>
                <gmd:CI_Contact>
                    <gmd:address>
                        <gmd:CI_Address>
                            <gmd:country>
                                <gco:CharacterString>Germany</gco:CharacterString>
                            </gmd:country>
                            <gmd:electronicMailAddress>
                                <gco:CharacterString>ops@eumetsat.int</gco:CharacterString>
                            </gmd:electronicMailAddress>
                        </gmd:CI_Address>
                    </gmd:address>
                    <gmd:onlineResource>
                        <gmd:CI_OnlineResource>
                            <gmd:linkage>
                                <gmd:URL>http://www.eumetsat.int</gmd:URL>
                            </gmd:linkage>
                        </gmd:CI_OnlineResource>
                    </gmd:onlineResource>
                </gmd:CI_Contact>
            </gmd:contactInfo>
            <gmd:role>
                <gmd:CI_RoleCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_ScopeCode" codeListValue="pointOfContact">pointOfContact</gmd:CI_RoleCode>
            </gmd:role>
        </gmd:CI_ResponsibleParty>
```

```
    </gmd:pointOfContact>
```

Temporal Extent

9.1.5 Product Temporal Information	
TEMPLATE Value:	ADD-TEMPORAL-INFORMATION *HR ADD-TEMPORAL-INFORMATION-startDate*HR, ADD-TEMPORAL-INFORMATION-endDate*HR
Information:	Time period to which the product applies
Necessity:	Optional for WMO Core Profile 1.3
Category:	Product information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/ gmd:extent/*/gmd:temporalElement/*/gmd:extent/*

This element describes the period of time that the available product covers. Where the product has a clear start and end date, and where the entire set of data is available, the specific start Date and end Date should both contain a date or dateTime. The date information is constructed as YYYY-MM-DD; while the date and time information is constructed as YYYY-MM-DDTHH:MM:SSZ (for UTC time). For example: 2016-04-17T13:42:54Z.

The following temporal Extents examples are described:

(a) **[DateX]** to **[DateY]** e.g. start Date:2005-10-01 end Date:2014-10-20

(b) **[DateX]** to **[Now]** e.g. start Date:2005-10-01 end Date:Now

(c) **[Now]** plus **[period]** e.g. start Date:now end Date:after duration: P1M (+1 month)

Where it is not possible to accurately capture (using start Date, end Date and duration) in the temporalExtent, then record details that are as close as possible, and then explain it in words, using the "description" field.

(a) [DateX] to [DateY] e.g. start Date:2005-10-01 end Date:2014-10-20

The following example shows a dataset with a known start date and a known end date

```
<gmd:temporalElement>
  <gmd:EX_TemporalExtent id="boundingTemporalExtent">
    <gmd:extent>
      <gml:TimePeriod gml:id="boundingTemporalExtentPeriod">
        <gml:beginPosition>2005-10-01</gml:beginPosition>
        <gml:endPosition>2014-10-20</gml:endPosition>
      </gml:TimePeriod>
    </gmd:extent>
  </gmd:EX_TemporalExtent>
</gmd:temporalElement>
```

(b) [DateX] to [now] e.g. start Date:2005-10-01 end Date:now

It is also possible to describe an on-going dataset with a known start date, but no known end Date. In that case, then end Date should contain the attribute of indeterminatePosition="now". For instance, where a dataset is from 2005-10-01 onwards, it would be encoded as follows :

```
<gmd:temporalElement>
  <gmd:EX_TemporalExtent id="temporalExtent">
    <gmd:extent>
      <gml:TimePeriod gml:id="boundingTemporalExtentPeriod">
        <gml:beginPosition>2005-10-01</gml:beginPosition>
        <gml:endPosition indeterminatePosition="now"/>
      </gml:TimePeriod>
    </gmd:extent>
  </gmd:EX_TemporalExtent>
</gmd:temporalElement>
```

The temporalExtent **options**, for a timePeriod, include beginPosition, endPosition and duration, e.g.:

```
<gml:beginPosition>   ..        …      …</gml:beginPosition>
<gml:endPosition>    ..          …       …</gml:endPosition>
<gml:duration> ..    …  …</gml:duration>
```

For a timePeriod, the **begin** and **end** Positions must always be included, and **duration** is optional.

The encoding of duration [(- or +) PnYnMnDTnhnmns] allows the expression of time intervals such as:

A number of years (nY), and/or months (nM), and/or (nD) days, or hours (nh), or minutes (nm), or seconds (ns), where "n" represents a number.

For example: a duration of 4 hours is expressed as **P0Y0M0DT4h0m0s** or **PT4h** Note that duration can be expressed as either the long form (eg P0Y5M0DT0h0m0s) or short form, but the short form must include "T" for intervals of hours, minutes or seconds (e.g. P5M is 5 months, PT5m is 5 minutes).

For more information on encoding a 'duration', see the "Durations" segment, at https://en.wikipedia.org/wiki/ISO_8601.

(b) [Now] plus [period] e.g. start Date:now end Date:after duration: P0Y0M7DT0h0m0s (+7 days)

For a dataset which is ongoing (that is, new data is continuously produced), but for which only the latest file is available (e.g. data is only ever available for a "rolling" window of time), the temporaExtent should reflect the period covered by the available data, in this case, the period that the latest file covers.

For instance, where only the latest file is ever available, and the latest file is a forecast for the next 7 days, it would be encoded as follows:

```
<gmd:temporalElement>
   <gmd:EX_TemporalExtent>
      <gmd:extent>
         <gml:TimePeriod>
            <gml:description>Next 7 days only</gml:description>
            <gml:beginPosition indeterminatePosition="now"/>
            <gml:endPosition indeterminatePosition="after"/>
            <gml:duration>P7D</gml:duration>
         </gml:TimePeriod>
      </gmd:extent>
   </gmd:EX_TemporalExtent>
</gmd:temporalElement>
```

Geographic Information

9.1.6 Geographical Information	
TEMPLATE Value:	(ADD-GEOSPATIAL-INFORMATION*C) ADD-BBOX-VALUE-WEST*M--MW, ADD-BBOX-VALUE-EAST*M-MW, ADD-BBOX-VALUE-SOUTH*M-MW, ADD-BBOX-VALUE-NORTH*M-MW
Information:	Geographic coverage of the product, as a bounding box in Latitude/Longitude
Necessity:	Conditional - Is Mandatory for WMO Core Profile 1.3, if the data is geographical
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:extent/*/gmd:geographicElement/ gmd:EX_GeographicBoundingBox/*/*/text() [having 4 elements]*

Geographical area covered by the data product. The geographical area is described as a bounding box with latitude and longitude in decimal degrees.

The following example shows the XML for a dataset's bounding box information :

```
<gmd:geographicElement>
   <gmd:EX_GeographicBoundingBox id="boundingGeographicBoundingBox">
      <gmd:westBoundLongitude>
         <gco:Decimal>-180</gco:Decimal>
      </gmd:westBoundLongitude>
      <gmd:eastBoundLongitude>
         <gco:Decimal>180</gco:Decimal>
      </gmd:eastBoundLongitude>
```

```
      <gmd:southBoundLatitude>
         <gco:Decimal>-90</gco:Decimal>
      </gmd:southBoundLatitude>
      <gmd:northBoundLatitude>
         <gco:Decimal>90</gco:Decimal>
      </gmd:northBoundLatitude>
   </gmd:EX_GeographicBoundingBox>
</gmd:geographicElement>
```

Bounding boxes that cross the 180 degree meridian can be differentiated from bounding boxes that do not, by the following rule:

- In a dataset that does not cross the 180 degree meridian, the western-most longitude shall always be less than the eastern-most longitude;
- Conversely, if a bounding box crosses the 180 degree meridian, then the western-most longitude shall be greater than the eastern-most longitude.

Other constraints on geographic bounding boxes:

- Geographic points shall be designated with the northern-most and southern-most longitudes equal, and the western-most and eastern-most longitudes equal;
- Except for a geographic point, the total longitudinal span shall be greater than zero, and less than or equal to 360 degrees;
- The northern-most latitude shall always be greater than or equal to than the southern-most latitude;
- Longitude and latitude shall be recorded in a coordinate reference system that has the same axes, units and prime meridian as WGS84.

Geographic Identifier

9.1.7 Geographic Identifier	
TEMPLATE Value:	(ADD-GEOGRAPHIC-IDENTIFIER INFORMATION *O) ADD-GEOGRAPHIC-IDENTIFIER-THESAURUS-NAME*O, ADD-GEOGRAPHIC-IDENTIFIER-CODE*C-MW
Information:	Geographic Identifier indicating the zone covered on earth by the product
Necessity:	Optional
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:extent/*/gmd:geographicElement/*/gmd:geographicIdentifier/gmd:MD_Identifier/code/*/text()*

Optional geographic identifier, indicating the area covered by the product. This can be used when the identifier is a well-known (within a targeted user community) or codified acronym for an area (such as a region), or feature (such as a water storage, coastline section, etc.). If the GeographicIdentifier block is used, then a code must be provided.

The GeographicIdentifier can be expressed in 2 ways:

(a) With just the Geographic Identifier Code, and a link to the related Codelist [Authority])

```
<gmd:extent>
   <gmd:EX_Extent id="geographicExtent">
      <gmd:geographicElement>
         <gmd:EX_GeographicDescription id="SouthAustralia__allGensRegister">
            <gmd:geographicIdentifier>
               <gmd:MD_Identifier>
                  <gmd:code>
                     <gco:CharacterString>
                           South Australia (SA)
                           (http://find.ga.gov.au/FIND/profileinfo/anzlic-allgens.xml#SA )
                     </gco:CharacterString>
                  </gmd:code>
               </gmd:MD_Identifier>
            </gmd:geographicIdentifier>
         </gmd:EX_GeographicDescription>
      </gmd:geographicElement>
   </gmd:EX_Extent>
</gmd:extent>
```

(b) With the Geographic Identifier Code, as well as a link to the related Codelist (via "Citation").

```
<gmd:extent>
   <gmd:EX_Extent id="geographicExtent">
      <gmd:geographicElement>
         <gmd:EX_GeographicDescription id="SouthAustralia__allGensRegister">
            <gmd:geographicIdentifier>
               <gmd:MD_Identifier>


                  <gmd:authority>
                     <gmd:CI_Citation>
                        <gmd:title>
                           <gco:CharacterString>
                           ANZLIC Geographic Extent Name Register
                           (http://find.ga.gov.au/FIND/profileinfo/anzlic-allgens.xml )
```

```
                        </gco:CharacterString>

                    </gmd:title>

                    <gmd:alternateTitle>

                        <gco:CharacterString>
                        ANZLIC      AllGens      /      subcategory:      anzlic-sla_2001edition
                        </gco:CharacterString>

                    </gmd:alternateTitle>

                    <gmd:date>

                        <gmd:CI_Date>

                            <gmd:date>

                                <gco:Date>2011-10-25</gco:Date>

                            </gmd:date>

                            <gmd:dateType>

                                <gmd:CI_DateTypeCode
codeList="http://www.isotc211.org/2005/resources/Codelist/gmxCodelists.xml#CI_DateTypeCode"
codeListValue="revision">revision</gmd:CI_DateTypeCode>

                            </gmd:dateType>

                        </gmd:CI_Date>

                    </gmd:date>

                </gmd:CI_Citation>

            </gmd:authority>


            <gmd:code>

                <gco:CharacterString>South                    Australia                    (SA)
                    (http://find.ga.gov.au/FIND/profileinfo/anzlic-allgens.xml#SA )

                </gco:CharacterString>

            </gmd:code>


        </gmd:MD_Identifier>

    </gmd:geographicIdentifier>

</gmd:EX_GeographicDescription>

</gmd:geographicElement>

</gmd:EX_Extent>

</gmd:extent>
```

Station Identifiers for GTS bulletins

References in WIS metadata records, to Stations for a GTS bulletin, should point to WIGOS station identifiers (available through OSCAR/surface), and should be provided as keywords. See: **Section 9.1.8 (ii)**.

Descriptive keywords

9.1.8 Descriptive Keywords

Descriptive keywords are additional "controlled" terms which further classify (and so increase searching accuracy for) the products. The following general rules apply, for keywords in a WMCP record:

- Terms from the same keyword thesaurus/codelist, and of the same KeywordTypeCode, shall be grouped into a single instance of the <gmd:descriptiveKeywords> class;
- All WMO Core Profile metadata records shall have a least one WMO CategoryCode keyword, and the related KeywordTypeCode will be 'theme';
- All WMCP records for GTS data must contain a keyword from the WMO_DistributionScopeCode codelist, and it must be accompanied by the KeywordTypeCode of "dataCentre";
- A WMP metadata record describing data for global exchange via the WIS* shall indicate the scope of distribution using the keyword “GlobalExchange” of type “dataCentre”;
- Where data is related to WMO stations, the related WIGOS Station Identifiers should be recorded as keywords, see 9.1.8 (iii);
- Any 'Data parameter' term added as a keyword should be accompanied by the KeywordTypeCode of "dataParam".

WMO Category Code Keyword

9.1.8 (i) WMO CategoryCode Keyword	
TEMPLATE Value:	WCMP-WMO-CATEGORY-CODE*M
Information:	One or more WMO Category keywords, for classifying the product.
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/ */gmd:descriptiveKeywords/*/gmd:keyword/*/ text()* */gmd:MD_Metadata/gmd:identificationInfo/ */gmd:descriptiveKeywords/*/ gmd:type/*/@codeListValue=”theme”* */gmd:MD_Metadata/gmd:identificationInfo/ */gmd:descriptiveKeywords/*/gmd:thesaurusName/ */ gmd:title/*/ text() =“WMO_CategoryCode*

Any WMO Core Profile metadata record shall have a least one WMO CategoryCode keyword, and the related KeywordTypeCode will be 'theme'.

The WMO CategoryCode list of terms is occasionally revised. For the latest list of terms, see:

http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_CategoryCode

At the time of writing, the WMO_CategoryCode list of terms includes:

WMO_CategoryCode	Term
WMO_CategoryCode_weatherObservations	weatherObservations
WMO_CategoryCode_weatherForecasts	weatherForecasts
WMO_CategoryCode_meteorology	Meteorology
WMO_CategoryCode_hydrology	Hydrology

WMO_CategoryCode	Term
WMO_CategoryCode_climatology	climatology
WMO_CategoryCode_landMeteorologyClimate	landMeteorologyClimate
WMO_CategoryCode_synopticMeteorology	synopticMeteorology
WMO_CategoryCode_marineMeteorology	marineMeteorology
WMO_CategoryCode_agriculturalMeteorology	agriculturalMeteorology
WMO_CategoryCode_aerology	aerology
WMO_CategoryCode_marineAerology	marineAerology
WMO_CategoryCode_oceanography	oceanography
WMO_CategoryCode_landHydrology	landHydrology
WMO_CategoryCode_rocketSounding	rocketSounding
WMO_CategoryCode_pollution	pollution
WMO_CategoryCode_waterPollution	waterPollution
WMO_CategoryCode_landWaterPollution	landWaterPollution
WMO_CategoryCode_seaPollution	seaPollution
WMO_CategoryCode_landPollution	landPollution
WMO_CategoryCode_airPollution	airPollution
WMO_CategoryCode_glaciology	glaciology
WMO_CategoryCode_actinometry	actinometry
WMO_CategoryCode_satelliteObservation	satelliteObservation
WMO_CategoryCode_airplaneObservation	airplaneObservation
WMO_CategoryCode_observationPlatform	observationPlatform
WMO_CategoryCode_spaceWeather	spaceWeather
WMO_CategoryCode_atmosphericComposition	atmosphericComposition
WMO_CategoryCode_radiation	Radiation

The example encoding below, for a satellite product, uses the terms "satelliteObservation" and "meteorology" as keywords from the WMO_CategoryCode thesaurus/codelist:

```
<gmd:descriptiveKeywords>
  <gmd:MD_Keywords>
    <gmd:keyword>

      <gco:CharacterString>satelliteObservation</gco:CharacterString>
    </gmd:keyword>

    <gmd:keyword>

      <gco:CharacterString>meteorology</gco:CharacterString>
    </gmd:keyword>
    <gmd:type>
            <MD_KeywordTypeCode     xmlns="http://www.isotc211.org/2005/gmd"     codeListValue="theme"
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_KeywordTypeCode">Theme</MD_KeywordTypeCode>
    </gmd:type>
    <gmd:thesaurusName>
            <gmd:CI_Citation>
          <gmd:title>
             <gco:CharacterString>WMO_CategoryCode</gco:CharacterString>

             </gmd:title>
             <gmd:date>
               <gmd:CI_Date>
                       <gmd:date>
                          <gco:Date>2016-04-01</gco:Date>
                       </gmd:date>
```

```
                    <gmd:dateType>
                          <gmd:CI_DateTypeCode                          codeListValue="publication"
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#CI_DateTypeCode"/>
                        </gmd:dateType>
                </gmd:CI_Date>
            </gmd:date>
          </gmd:CI_Citation>
      </gmd:thesaurusName>
    </gmd:MD_Keywords>
</gmd:descriptiveKeywords>
```

WMO Distribution Scope Keyword

9.1.8 (ii) WMO Distribution Scope Code Keyword	
TEMPLATE Value:	ADD-DISTRIBUTION-SCOPE*C
Information:	Scope of distribution of data within the WMO Information System.
Necessity:	Conditional. Mandatory for WMO Core Profile 1.3, for GTS data.
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/*@codeListValue=" dataCentre"* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:thesaurusName/*/ gmd:title/*/text() ="WMO_DistributionScopeCode"*

Any WMCP record for GTS data must contain a DistributionScopeCode keyword. The scope of distribution, for data within WIS, shall be expressed as a keyword, using a term from the "WMO_DistributionScopeCode", and that keyword shall have a **KeywordTypeCode** of "datacentre". The keyword will be one of the following terms (from the controlled vocabulary called "WMO_DistributionScopeCode"):

- GlobalExchange,
- RegionalExchange,
- OriginatingCentre.

A WIS Discovery Metadata record describing data for global exchange via the WIS shall have a keyword "GlobalExchange", of KeywordTypeCode "dataCentre", from the thesaurus of "WMO_DistributionScopeCode"; it must also include a term from both the WMO_DataLicenseCode and WMO_GTSProductCategoryCode within the resourceConstraints section of the record (see Section 9.1.10, for details).

The GTS (Global Telecommunication System) is the part of the WIS that is concerned with rapid, near-real time information exchange. GISCs are required to retain at least 24h of information exchanged globally using the GTS.

The keyword term from the codelist called WMO_DistributionScopeCode is used to indicate whether the product described by a metadata record is or isn't delivered via the GTS and GISCS, and, within the GTS, whether it is exchanged globally or regionally.

- Metadata marked **GlobalExchange** or **RegionalExchange** describes data delivered via the GTS. Data is transmitted from an originating NC/DCPC to the principal GISC, distributed to all (or some) GISCs, then placed on the GISC caches;

- Metadata marked **RegionalExchange**, is for data that, while transmitted on the GTS, might be simply exchanged between two WMO Members (by bilateral agreement). Some example data are regional warnings, or voluminous NWP products;

- The metadata marked **OriginatingCentre** indicates 'non-GTS data', and includes, for instance, data delivered to users from a DCPC.

Below is an example for 'globally exchanged' GTS data:

```
<gmd:descriptiveKeywords>

    <gmd:MD_Keywords>

        <gmd:keyword>

            <gco:CharacterString>GlobalExchange</gco:CharacterString>

        </gmd:keyword>

        <gmd:type>

            <gmd:MD_KeywordTypeCode
codeList="http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#MD_KeywordTypeCode"
codeListValue="dataCentre">dataCentre</gmd:MD_KeywordTypeCode>

        </gmd:type>

        <gmd:thesaurusName>

            <gmd:CI_Citation>

                <gmd:title>

                    <gco:CharacterString>WMO_DistributionScopeCode
[http://wis.wmo.int/2012/codelists/WMOCodeLists.xml]</gco:CharacterString>

                </gmd:title>

                <gmd:date>

                    <gmd:CI_Date>

                        <gmd:date>

                            <gco:Date>2012-06-27</gco:Date>

                        </gmd:date>

                        <gmd:dateType>

                            <gmd:CI_DateTypeCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/codel
ist/gmxCodelists.xml#CI_DateTypeCode" codeListValue="revision">revision</gmd:CI_DateTypeCode>

                        </gmd:dateType>

                    </gmd:CI_Date>

                </gmd:date>

            </gmd:CI_Citation>

        </gmd:thesaurusName>

    </gmd:MD_Keywords>

</gmd:descriptiveKeywords>
```

WIGOS Station Identifier Keyword

9.1.8 (iii) WIGOS Station Identifiers Keywords	
TEMPLATE Value:	ADD-WIGOS-STATION-IDENTIFIER-CODE*O; ADD-WIGOS-STN-ID-CODE-AUTHORITY*O;
Information:	Where a product includes data from Stations which have been assigned a WIGOS Station Identifier, include these as keywords
Necessity:	Optional for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/* *@codeListValue="place"* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:thesaurusName/*/* *gmd:title/*/text()="WMO WIGOS Station Identifiers"*

Where products include data from Stations which have been assigned a WIGOS Station Identifier, include these as keywords. Where metadata records previously included WMO Station numbers as keywords, the WIGOS Station Identifier should now be used. The related **KeywordTypeCode** should be "place".

Below is example encoding of WIGOS Station Identifiers, as keywords

```
<gmd:descriptiveKeywords>
   <gmd:MD_Keywords>
       <gmd:keyword>

         <gco:CharacterString>
          0-20000-0-94287;    CAIRNS    AERO    [    http://data.wmo.int/wigosid=0-20000-0-94287    ]
         </gco:CharacterString>
      </gmd:keyword>
       <gmd:keyword>

         <gco:CharacterString>
          0-20000-0-94374;   ROCKHAMPTON     AERO   [   http://data.wmo.int/wigosid=0-20000-0-94374   ]
         </gco:CharacterString>
      </gmd:keyword>
       <gmd:keyword>

         <gco:CharacterString>
          0-20000-0-94294;   TOWNSVILLE    AERO   [   http://data.wmo.int/wigosid=0-20000-0-94294   ]
         </gco:CharacterString>
      </gmd:keyword>


       <gmd:type>
          <gmd:MD_KeywordTypeCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/codel
ist/gmxCodelists.xml#MD_KeywordTypeCode"              codeListValue="place"</gmd:MD_KeywordTypeCode>
       </gmd:type>

       <gmd:thesaurus>
          <gmd:CI_Citation>
             <gmd:title>
                  <gco:CharacterString>WMO WIGOS Station Identifiers</gco:CharacterString>

             </gmd:title>


              <gmd:date>

                 <gmd:CI_Date>

                    <gmd:date>

                       <gco:Date>2016-06-25</gco:Date>
```

```
                    </gmd:date>

                 <gmd:dateType>

                     <gmd:CI_DateTypeCode
codeList="http://www.isotc211.org/2005/resources/Codelist/gmxCodelists.xml#CI_DateTypeCode"
codeListValue="revision">revision</gmd:CI_DateTypeCode>

                 </gmd:dateType>

              </gmd:CI_Date>

           </gmd:date>


       </gmd:CI_Citation>
    </gmd:thesaurus>
  </gmd:MD_Keywords>
</gmd:descriptiveKeywords>
```

Data Parameters

9.1.8 (iv) Data Parameter Keyword	
TEMPLATE Value:	ADD-DATA-PARAMETER*O
Information:	Data parameter keywords, for classifying the product.
Necessity:	Optional for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:keyword/*/text()* */gmd:MD_Metadata/gmd:identificationInfo/*/gmd:descriptiveKeywords/*/gmd:type/*/@codeListValue="dataParam"*

Where feasible, a list of the data parameters may be added as keywords. These should be added under a separate 'descriptiveKeywords' block, and should use the **KeywordTypeCode** of 'dataParam'.

Below is example encoding of a Data Parameter as a keyword.

```
<gmd:descriptiveKeywords>
   <gmd:MD_Keywords>
      <gmd:keyword>

         <gco:CharacterString>Dewpoint temperature</gco:CharacterString>

      </gmd:keyword>

       <gmd:type>
          <gmd:MD_KeywordTypeCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/codelist/gmxCodelists.xml#MD_KeywordTypeCode"                    codeListValue="dataParam">dataParam</gmd:MD_KeywordTypeCode>
       </gmd:type>


       <gmd:thesaurus>
          <gmd:CI_Citation>
             <gmd:title>
                <gco:CharacterString>WMO              Grib2              parameter              list
http://codes.wmo.int/grib2/codeflag/4.2/                                    </gco:CharacterString>
             </gmd:title>
```

```
            <gmd:date>

               <gmd:CI_Date>

                  <gmd:date>

                     <gco:Date>2016-06-25</gco:Date>

                  </gmd:date>

               <gmd:dateType>

                  <gmd:CI_DateTypeCode
codeList="http://www.isotc211.org/2005/resources/Codelist/gmxCodelists.xml#CI_DateTypeCode"
codeListValue="revision">revision</gmd:CI_DateTypeCode>

               </gmd:dateType>

            </gmd:CI_Date>

         </gmd:date>


      </gmd:CI_Citation>
   </gmd:thesaurus>
  </gmd:MD_Keywords>
</gmd:descriptiveKeywords>
```

Product Sample Visualization URL

9.1.9 Product Sample Visualization URL	
TEMPLATE Value:	ADD-PRODUCT-IMAGERY-URL*O
Information:	URL to a sample data visualization
Necessity:	Optional for WMO Core Profile 1.3, but used by WIS Portal to display products
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:graphicOverview/*/gmd:fileName/*/text()*

The addition of a link to the product visualization is suggested, when possible. The display of related linked images can make the products more attractive for end users.

Below is an example, based on EUMETSAT Seviri Level 1.5.

```
<gmd:graphicOverview>
   <gmd:MD_BrowseGraphic>
      <gmd:fileName>

         <gco:CharacterString>http://navigator.eumetsat.int:80/smartEditor/preview/msg-level-1-
5.jpg</gco:CharacterString>
      </gmd:fileName>
      <gmd:fileDescription>
         <gco:CharacterString>preview</gco:CharacterString>
      </gmd:fileDescription>
      <gmd:fileType>
         <gco:CharacterString>jpg</gco:CharacterString>
      </gmd:fileType>
   </gmd:MD_BrowseGraphic>
</gmd:graphicOverview>
```

Data Policy Information

Data Policy Information	
TEMPLATE Value:	ADD-DATA-POLICY-CODE*C
Information:	Data usage and limitations to access the resource

Necessity:	Mandatory for WMO Core Profile 1.3, for data intended for Global Exchange on the GTS. Otherwise, highly recommended, since the absence of a policy can result in users assuming that there are no limitations on Data use. To avoid uncertainty, where there ARE no limitations, use the Data Policy of "NoLimitation".
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:resourceConstraints/gmd:MD_LegalConstraints/*↘ {complex content}, including ↘ */gmd:otherConstraints/*/text()=WMO_DataLicenseCode* and ↘ */gmd:otherConstraints/*/text()=WMO_GTSProductCategoryCode*

The Data Policy category is used to specify the conditions under which the data products can be accessed and used. Completing the data policy section of a WMO Core Profile metadata record is very dependent on the type of data, data policy and the different ways that the data is being distributed. For those reasons, and to minimize the complexity of this section, three representative examples, covering some typical data policies - are presented below.

- Example 1: Non GTS Product, with a policy of no constraints on use or distribution;
- Example 2: Non GTS Product, with a policy applicable in the WMO context;
- Example 3: GTS Data, Intended for Global Exchange.

For a more comprehensive documentation, please refer to the documentation of the WMO Core Profile contained in the Manual on WIS.

When adding the data policy information, two different parts of the metadata record have be filled:

- The **resourceConstraints** part, which contains the data policy information; and
- The **scope of distribution** part: using one of the terms: 'GlobalExchange', 'RegionalExchange' or 'OriginatingCentre' (to be inserted as a keyword, as explained in Section 9.1.8 (ii)).

Each of the 3 examples below present the first part of the above information (**resourceConstraints**), that is to be added.

Within the the **resourceConstraints** section, the DataLicenseCode term is added into an 'otherConstraints' field; and an explanation of the Data Policy is typically added to an additional 'otherConstraints' field.

```
/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:resourceConstraints/gmd:MD_L
egalConstraints/gmd:otherConstraints/*/text()
```

Allowable terms from the DataLicenseCode include: "WMOAdditional", "WMOEssential", "WMOOther" or "NoLimitation". All of these terms are defined at http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_DataLicenseCode

Example 1 details: Non GTS Product, with a policy of no constraints on use or distribution

Publicly available datasets are datasets where no conditions and restrictions apply, on data access and data usage.

The 'useLimitation' field in the 'resourceConstraints' block should contain “No conditions apply”, and an 'otherConstraints' field should contain the phrase “NoLimitation”.

```
<!-- Example of publicly available, unrestricted data -->

<gmd:resourceConstraints>

  <gmd:MD_LegalConstraints>

    <!--  add useLimitation with ..No conditions apply..  -->

    <gmd:useLimitation>

      <gco:CharacterString>No conditions apply</gco:CharacterString>

    </gmd:useLimitation>

    <gmd:useConstraints>

      <!--  Restriction code have to point to WMOCodeLists.xml -->

<gmd:MD_RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"

         codeListValue="otherRestrictions">otherRestrictions</gmd:MD_RestrictionCode>

    </gmd:useConstraints>

    <!--  otherConstraints with ..NoLimitation..  -->

    <gmd:otherConstraints>

      <gco:CharacterString>NoLimitation</gco:CharacterString>

    </gmd:otherConstraints>

  </gmd:MD_LegalConstraints>

</gmd:resourceConstraints>
```

In addition, the **scope of distribution** would also ideally be stated (as a keyword), and for non GTS products it should be 'OriginatingCentre'

```
<!-- Scope of distribution for non GTS products: OriginatingCentre -->

<gmd:descriptiveKeywords>

  <gmd:MD_Keywords>

    <gmd:keyword>

      <!--  keyword OriginatingCentre applies for DCPC Data -->

      <gco:CharacterString>OriginatingCentre</gco:CharacterString>

    </gmd:keyword>

    <gmd:type>

      <gmd:MD_KeywordTypeCode
           codeList="http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#MD_DistributionScopeCode"

           codeListValue="dataCentre">dataCentre</gmd:MD_KeywordTypeCode>
```

```
    </gmd:type>

    <gmd:thesaurusName>

      <gmd:CI_Citation>

        <gmd:title>

          <gco:CharacterString>WMO_DistributionScopeCode,  WMOCodelists  dictionary  Version  1.3
[http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_DistributionScopeCode]</gco:CharacterString>

        </gmd:title>

    .. .. .. etc    (see Section 9.1.8 (ii) for full details
```

Example 2 details: Non GTS Product, with a policy applicable in the WMO context

This example describes a data product that is not distributed on the GTS, and which has a single data policy applicable in the WMO context. Note that policies that are applicable in the WMO context (and therefore flagged, in an 'otherConstraints' field, with the term "WMOOther") will be presented by the GISCs to the users when they discover the data. GISCs have no obligations to show the other data policies.

A term from the **WMO_DataLicenseCode** codelist, http://wis.wmo.int/2012/metadata/version_1-3/WMOCodelists.xml#WMO_DataLicenseCode, should be added to an 'otherConstraints' field.

Note: The Data Policy term of "WMOOther" can also be used for data that is delivered via the GTS.

```
<gmd:resourceConstraints>

  <gmd:MD_LegalConstraints>

    <!--   Add useLimitation to indicate the limitations of usage for the data  -->

      <gmd:useLimitation>

        <gco:CharacterString>Disclaimer - While every effort has been made to ensure that these data
are accurate and reliable within the limits of the current state of the art, OrganisationX cannot
assume liability for any damages caused by any errors or omissions in the data, nor as a result of
the failure of the data to function on a particular system. OrganisationX makes no warranty,
expressed or implied, nor does the fact of distribution constitute such a warranty.

        </gco:CharacterString>

      </gmd:useLimitation>

      <gmd:accessConstraints>

<gmd:MD_RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="copyright">copyright</gmd:MD_RestrictionCode>

      </gmd:accessConstraints>

      <gmd:accessConstraints>

         <gmd:MD_RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="otherRestrictions">otherRestrictions</gmd:MD_RestrictionCode>

      </gmd:accessConstraints>
```

```
      <gmd:useConstraints>

        <gmd:MD_RestrictionCode

codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="copyright">copyright</gmd:MD_RestrictionCode>

      </gmd:useConstraints>

      <gmd:useConstraints>

         <gmd:MD_RestrictionCode

codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="otherRestrictions">otherRestrictions</gmd:MD_RestrictionCode>

      </gmd:useConstraints>

      <!--  Add WMOOther, to signal that the policy is applicable in the WMO Context -->

      <gmd:otherConstraints>

         <gco:CharacterString>WMOOther

Ordnance Survey Open Data License [https://www.ordnancesurvey.co.uk/docs/licences/os-opendata-licence.pdf]
         </gco:CharacterString>

      </gmd:otherConstraints>

   </gmd:MD_LegalConstraints>

</gmd:resourceConstraints>
```

The scope of distribution, using the term 'OriginatingCentre' would also, ideally, be added (as a keyword).

Please refer to the example encoding of 'scope of distribution', provided (above) under Example 1 above, or in Section 9.1.8 (ii).

Example 3 details: GTS Data, Intended for Global Exchange

This example describes data distributed via the GTS and available from the cache at a GISC. For data that are delivered via the GTS, the data policy term to be added to the 'otherConstraints' field can only be "WMOAdditional" or "WMOEssential" – both of these terms are defined at http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_DataLicenseCode.

In the example below, the code is 'WMOEssential'.

WMO data policies (licence conditions) are defined by Resolution 40 (Cg-XII), Resolution 25 (Cg-XIII) and Resolution 60 (Cg-17) for data and products. Free and unrestricted basis data are "WMOEssential"; data classed as having a data policy of "WMOAdditional" have restrictions on commercial activities. Operational meteorological information for aviation is not included in these resolutions, but is controlled by ICAO; these data are an example of "WMOOther" data.

Only one term from the **WMO_DataLicenseCode** may be used, within a metadata record. As well as assigning one of these terms, it is expected, where the term used is "WMOOther" or

"WMOAdditional", that further clarification of thelLicence constraints will also be provided (either directly in the metadata record, or else via a URL).

For data circulating on the GTS, "WMOAdditional" is used to qualify products under the “WMO Additional” data policy, "WMOEssential" is used for products made available under the “WMO Essential” data policy, and "WMOOther" can be applied (where applicable) for other products , regardless of whether the data is being delivered via the GTS/GISC or otherwise.

Where data is for GlobalExchange on the GTS (which is signified by the WMO_DistributionScopeCode Keyword), both a **WMO_DataLicenseCode** and a **WMO_GTSProductCategoryCode** term must be provided, under ResourceConstraints. The choice of terms, from the **WMO_GTSProductCategoryCode** codelist, are: "GTSPriority1", "GTSPriority2", "GTSPriority3", "GTSPriority4".

Below is the resourceConstraints element for a "WMOEssential" GTS product, intended for global exchange:

```
<!--   Data intended for WMOEssential data intended for Global exchange -->

<gmd:resourceConstraints>

   <gmd:MD_LegalConstraints>

      <gmd:useLimitation>

        <gco:CharacterString>Data is near realtime, and is not quality controlled. License
conditions apply, as indicated below</gco:CharacterString>

      </gmd:useLimitation>

      <!--   MD_RestrictionCode to be ‘otherRestrictions’ -->

      <gmd:accessConstraints>

<gmd:MD_RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_RestrictionCode"  codeListValue="copyright">copyright</gmd:MD_RestrictionCode>

      </gmd:accessConstraints>

      <gmd:accessConstraints>

         <gmd:MD_RestrictionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="otherRestrictions">otherRestrictions</gmd:MD_RestrictionCode>

      </gmd:accessConstraints>

      <gmd:useConstraints>

        <gmd:MD_RestrictionCode

codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="copyright">copyright</gmd:MD_RestrictionCode>

      </gmd:useConstraints>

      <gmd:useConstraints>

         <gmd:MD_RestrictionCode
```

```
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codelist/gmxCodelists.xml#MD_RestrictionCode"
codeListValue="otherRestrictions">otherRestrictions</gmd:MD_RestrictionCode>

      </gmd:useConstraints>



      <!-- Add WMO Data policy and GTSPriority -->

      <gmd:otherConstraints>

         <gco:CharacterString>WMOEssential    A  definition  of  "WMOEssential"  is  available  at:
http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#WMO_ DataLicenseCode </gco:CharacterString>

      </gmd:otherConstraints>

      <gmd:otherConstraints>

         <gco:CharacterString>GTSPriority2</gco:CharacterString>

      </gmd:otherConstraints>

   </gmd:MD_LegalConstraints>

</gmd:resourceConstraints>
```

In addition, the scope of distribution of "GlobalExchange" has to be added, as a keyword (with KeywordTypeCode of "dataCentre").

```
<!-- keyword for stating the scope of distribution: Global Exchange   -->

<gmd:descriptiveKeywords>

  <gmd:MD_Keywords>

    <gmd:keyword>

      <gco:CharacterString>GlobalExchange</gco:CharacterString>

    </gmd:keyword>

    <gmd:type>

      <gmd:MD_KeywordTypeCode
           codeList="http://wis.wmo.int/2012/codelists/WMOCodeLists.xml#MD_DistributionScopeCode"

           codeListValue="dataCentre">dataCentre</gmd:MD_KeywordTypeCode>

    </gmd:type>

  .. .. .. etc   (see Section 9.1.8 (ii), for full example
```

Distribution Information

9.1.11 Distribution Information	
TEMPLATE Value:	ADD-URL-TO-DATA-ACCESS-SERVICE*HR-MW, ADD-DISTRIBUTOR-SHORTNAME*HR (e.g.:EUM), ADD-DISTRIBUTOR-EMAIL-ADDRESS*HR, ADD-FORMAT-NAME*O-MW, ADD-FORMAT-VERSION*O-MW
Information:	Resource format, distributor information, and resource transfer options (urls)
Necessity:	Highly Recommended for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:distributionInfo/*/gmd:distributionFormat/*/gmd:formatDistributor/*/* {complex content}, including ↘*distributorContact/gmd:CI_ResponsibleParty/* and ↘*distributorTransferOptions/*/gmd:online/*

Below is an example for a GRIB product made available via FTP server (distributor details are not included in this snippet, for readability, but are included in the TEMPLATE record)

```
<gmd:distributionInfo>
    <gmd:MD_Distribution>
        <gmd:distributionFormat>
            <gmd:MD_Format>
                <gmd:name>
                    <gco:CharacterString>GRIB</gco:CharacterString>
                </gmd:name>
                <gmd:version>
                    <gco:CharacterString>FM 92 GRIB Edition 2</gco:CharacterString>
                </gmd:version>
                <gmd:specification>

<gco:CharacterString>http://www.wmo.int/pages/prog/www/WMOCodes.html</gco:CharacterString>
                </gmd:specification>
            </gmd:MD_Format>
        </gmd:distributionFormat>
        <gmd:transferOptions>
            <gmd:MD_DigitalTransferOptions>
                <gmd:onLine>
                    <gmd:CI_OnlineResource>
                        <gmd:linkage>
                            <gmd:URL>ftp://data-portal.ecmwf.int/</gmd:URL>
                        </gmd:linkage>
                        <gmd:protocol>
                            <gco:CharacterString>WWW:DOWNLOAD-1.0-ftp--download</gco:CharacterString>
                        </gmd:protocol>
                        <gmd:name>
                            <gco:CharacterString>ECMWF DCPC FTP Server</gco:CharacterString>
                        </gmd:name>
                        <gmd:description>
                            <gco:CharacterString>WMO Information System download service through
ECMWF DCPC</gco:CharacterString>
                        </gmd:description>
```

```
                        <gmd:function>

                            <gmd:CI_OnLineFunctionCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#CI_OnLineFunctionCode"
codeListValue="download">download</gmd:CI_OnLineFunctionCode>

                        </gmd:function>

                    </gmd:CI_OnlineResource>

                </gmd:onLine>

            </gmd:MD_DigitalTransferOptions>

        </gmd:transferOptions>

    </gmd:MD_Distribution>

</gmd:distributionInfo>
```

Party to be cited

9.1.12 Cited Party Information	
TEMPLATE Value:	ADD-CITED-RESPONSIBLE-PARTY-ORGANISATION*O-MW
Information:	Party that should be cited as the 'originator' [that is, data-author], for the resource
Necessity:	Optional for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:distributionInfo/*/gmd:citation/*/gmd:citedResponsibleParty/gmd:CI_ResponsibleParty/* {complex content}

Where the data owner wishes to be cited, in references made to their data, they can stipulate this in the citedResponsibleParty block, using a role of 'originator'

Below is an example:

```
<gmd:identificationInfo>

<gmd:MD_DataIdentification>

   <gmd:citation>

      <gmd:CI_Citation>

         …. .. .. ..

         <gmd:citedResponsibleParty>

            <gmd:CI_ResponsibleParty>

                <gmd:organisationName>

                    <gco:CharacterString>EUMETSAT</gco:CharacterString>

                </gmd:organisationName>

                <gmd:role>

                    <gmd:CI_RoleCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codel
ist/gmxCodelists.xml#MD_ScopeCode" codeListValue="pointOfContact">originator</gmd:CI_RoleCode>

                </gmd:role>

            </gmd:CI_ResponsibleParty>
```

```
        </gmd:citedResponsibleParty>

        <gmd:otherCitationDetails>

            <gco:CharacterString>Add other citing instructions here</gco:CharacterString>

        </gmd:otherCitationDetails>
          .. .. .. ..

      </gmd:CI_Citation>

    </gmd:citation>
     .. .. .. ..

  </gmd:MD_DataIdentification>

</gmd:identificationInfo>
```

Additional details on how the item should be cited can be added to the 'otherCitationDetails' block.

Resource Update frequency

9.1.13 Resource Update Frequency Information	
TEMPLATE Value:	ADD-PRODUCT-UPDATE-FREQ-PERIOD*O, ADD-PRODUCT-UPDATE-FREQ-CODE*O-MW
Information:	Frequency of resource update
Necessity:	Optional for WMO Core Profile 1.3
Category:	Product Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:resourceMaintenance/*/gmd:maintenanceAndUpdateFrequency/*

If the Resource Update frequency block is used, then the *MD_MaintenanceFrequencyCode* is mandatory.

The example below is for a product which is available every 6 hours, starting at 3 UTC

```
<gmd:resourceMaintenance>

   <gmd:MD_MaintenanceInformation>

      <gmd:maintenanceAndUpdateFrequency>

         <gmd:MD_MaintenanceFrequencyCode                                    codeListValue="irregular"
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/codelist/gmxCodelists.xml#MD_MaintenanceFrequencyCode"/>

      </gmd:maintenanceAndUpdateFrequency>

      <gmd:userDefinedMaintenanceFrequency>

         <gts:TM_PeriodDuration>PT6H</gts:TM_PeriodDuration>

      </gmd:userDefinedMaintenanceFrequency>

      <gmd:maintenanceNote>

         <gco:CharacterString>ADD-PRODUCT-UPDATE-FREQ-NOTE          (e.g.    Instances   of   bulletin
SIKB20NGTT are available every 6 hours starting at 03 UTC)</gco:CharacterString>

      </gmd:maintenanceNote>

   </gmd:MD_MaintenanceInformation>

</gmd:resourceMaintenance>
```

Mandatory WIS Technical Information

In addition to those mandatory elements included on section 9.1 above, the following information is required:

Metadata Record Unique Identifier

9.1.14 Metadata Record Unique Identifier	
TEMPLATE Value:	ADD-WMCP-IDENTIFIER*M
Information:	Unique Identifier for individual WIS Discovery Metadata Records
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	WIS Technical Information
XPath:	*/gmd:MD_Metadata/gmd:fileIdentifier/*/text()*

The WCMP UID (fileIdentifier) should be structured as

urn:x-wmo:md:DataProviderInternetDomainName::ProductUID

where:

"**:**" is used as a separator;

urn:x-wmo:md: is mandatory;

DataProviderInternetDomainName:: designates the citation authority based on the reversed Internet domain name of the data-provider organization (e.g. int.eumetsat, gov.noaa) – note the recommended use of two colons "**::**";

ProductUID is a unique identifier with a structure defined by the organization responsible for the metadata record.

Examples:

UID for Roshydromet MTVZA-GY Level 1C data Meteor-M N2:

```
urn:x-wmo:md:planet.iitp.ru:EO:ROSHDAT:METEOR-M:MTVZA-GY
```

EUMETSAT Meteosat Seviri Level 1.5:

```
urn:x-wmo:md:int.eumetsat:EO:EUM:DAT:MSG:HRSEVIRI
```

Unique Identifier for GTS products

Additional rules apply, for metadata records describing products distributed in the GTS. The file identifier for bulletin metadata has the following structure:

```
urn:x-wmo:md:int.wmo.wis::{uid}
```

where {uid} is a unique identifier derived from the GTS bulletin or file name.

Further background, on constructing a fileIdentifier for products distributed on the GTS, is available in the WMCP v.1.3, Part 1, Section 9.2 ("Identifiers for metadata describing data published for global exchange").

An example File Identifier for a Deutscher Wetterdienst Numerical Weather Prediction Model, GTS Bulletin is:

```
urn:x-wmo:md:int.wmo.wis::HTXC85EDZW
```

An example File Identifier Meteo France Numerical Weather Prediction Model is:

```
urn:x-wmo:md:int.wmo.wis::FR-meteofrance-toulouse,GRIB,ARPEGE-75N10N-60W65E_C_LFPW
```

Metadata modification DateStamp

9.1.15 Metadata Modification DateStamp	
TEMPLATE Value:	ADD-METADATA-LAST-MODIFICATION-DATE*M
Information:	Last modification date of the metadata record
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	WIS Technical Information
XPath:	*/gmd:MD_Metadata/gmd:dateStamp*

This is the metadata record's latest modification date, and is a DATETIME. It has the following date pattern: **YYYY-MM-DDThh:mm:ss**, for example 2015-12-29T11:45:55.

Product Creation Date

9.1.16 Creation Date	
TEMPLATE Value:	ADD-PRODUCT-CREATION-DATE*M
Information:	Creation date of the product
Necessity:	Mandatory for WMO Core Profile 1.3
Category:	WIS Technical Information
XPath:	*/gmd:MD_Metadata/gmd:identificationInfo/*/gmd:citation/*/gmd:date/*/* ↘ */gmd:date/*/text()* ***and*** ↘ */gmd:dateType/*/@codeListValue="creation"*

This is the product Creation date, and has the following date pattern: **YYYY-MM-DD** or **YYYY-MM-DDThh:mm:ss.**

For instance:

```
<gmd:date>
   <gmd:CI_Date>
      <gmd:date>
         <gco:Date>2015-03-23</gco:Date>
      </gmd:date>
      <gmd:dateType>
         <gmd:CI_DateTypeCode
codeList="http://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_19139_Schemas/resources/Codelist/gmxCodelists.xml#CI_DateTypeCode"                                codeListValue="creation"/>
      </gmd:dateType>
   </gmd:CI_Date>
<gmd:date>
```

Technical Document

More details on the WMO Core Profile Metadata can be found at http://wis.wmo.int/MD_Index

Annex

Glossary

- CGMS: Coordination Group for Meteorological Satellites
- CGMS-WMO TFMI: CGMS-WMO Task Force on Metadata Implementation
- GTS: Global Telecommunication Network
- WMO IPET-SUP: WMO Inter-Programme Expert Team on Satellite Utilization and Products
- WIS: WMO Information System
- GISC: Global Intercommunication System Centre
- DCPC: Data Collection and Production Centre
- NC: National Centre
- WMCP: WMO Core Profile
- ISO 19115: http://www.iso.org/iso/catalogue_detail?csnumber=26020

Collection Definition Criteria

This part of the document defines criteria and elements to consider, when creating a metadata record representing a collection of products.

To understand the notion of collection, it is important to distinguish between a dataset and a temporal subset of a dataset. As well, the availability of meteorological data is often transient (e.g. observations, forecasts, NWP products), and continuously updated. A dataset is typically seen as an aggregate of temporal "instances"/subsets of the same dataset (the collection) and, as explained below, metadata for a dataset is not typically set at "instance" level. This is so, even when a new instance/subset of a dataset is produced daily, and when only the latest day of data is ever available (in that case, the temporalExtent of the dataset is "latest 24 hours only").

Additional criteria can be considered, when creating the collection metadata record include :

(a) Size of dataset instances.

An important thing to consider, in terms of Dataset granularity, is how the dataset instances will be made available to end users. For instance, push or pull services, with filter capabilities or not.

Numerical model X output could be seen as a 4 and even 5-D dataset (latitude, longitude, Z, time, reference time). It is possible to set granularity at this level, but the amount of data will be huge, and it will not be possible to exchange the whole dataset, using 'push' mode: Such

large scale granularity of data is ideally provided via download (or publish-subscribe) services with sub setting capabilities (e.g. WCS, or "Direct" download INSPIRE services).

When the data provider is not able to implement such services, and when only pre-defined datasets or time-windows are made available (i.e., the use case of datasets for global exchange on the WIS) the granularity may have to be finer.

For example, the French high resolution model, AROME, is split into two daily subsets:

Dataset 1 : AROME 0°01 FRANCE - 00h-23h

Dataset 2 : AROME 0°01 FRANCE - 24h-45h

Where Dataset 1 covers hourly steps H to H+23h and Dataset 2 covers hourly steps H+24 to H+45.

The granularity of the subsets is chosen according to the size of the instances to be exchanged, and the size of the granules (500 Mb, 1Gb, ...) should be compatible with the bandwidth available for data exchange. Note that it is also possible to define an aggregate of the two subsets, for instance:

Dataset 0 : AROME 0°01 FRANCE, where Dataset 0 is an aggregation of Dataset 1 and Dataset 2.

(b) Content consistency

It is recommended, if possible, to not blend multiple data categories or topics in the same dataset, resulting in an heterogeneous aggregate.

For example an aggregate of satellite observations, and weather forecasts would not typically make sense (unless they had been combined for a particular purpose); whereas an aggregate of pollution and water pollution data makes sense, especially if the data processing has been similar and the data license is the same.

More generally, dataset heterogeneity in terms of content can result in very generalized descriptions in the metadata, which will, in turn, affect data discoverability on the WIS.

(c) Update frequency, other temporal characteristics

The refresh-rate of data also has to be taken into account, in terms of dataset granularity, because this will have an impact on catalogues.

Setting the dataset/metadata granularity at the "temporal instance" level, instead of "time series" level, would require the generation (automatically) of a lot of metadata records, and the update of catalogues in near real-time. It would also present difficulties in synchronizing metadata records among the GISCs, especially through harvesting processes. Such a large number of metadata records would also make it difficult for users to find the information they were seeking.

For instance, a "French WMO Resolution 40 Essential SYNOP" dataset could be seen as a temporal "series", and, provided that the entire dataset continues to be available, the discovery metadata should be provided at this level, and not at "temporal instance" level (e.g. "French WMO Resolution 40 Essential SYNOP 2016-04-07T12:00:00Z").

It is also recommended to not blend data of different refresh-rates in the same dataset, because it will not be possible to specify the update frequency in discovery metadata records.

(d) Data policy and distribution scope

A dataset shall be homogeneous in terms of data policy, including WMO distribution policy, which is described through WMO_DistributionScopeCode, WMO_DataLicenseCode, WMO_GTSProductCategoryCode and MD_RestrictionCode code lists.

The definition of the WCMP 1.3 mentions, in section 9.3 of Appendix C Part 1 of the Manual on WIS, that:

> "The presence of more than one WMO Data Policy in a single metadata record yields an ambiguous state, a WIS Discovery Metadata record describing data for global exchange shall declare only a single Data Policy".

Beyond WCMP 1.3 compliance, it is not easy to describe multiple data policies in a same metadata record, and if a dataset is heterogeneous in terms of data policy, the implementation of these policies by the services may be difficult.

(e) Spatial extent

Except for global datasets, a coarse granularity is likely to affect the discoverability of data on the basis of spatial criterion, especially if the effective areas where data is available are disjoint. For example synoptic observations for the French Overseas Departments of Guyana, Martinique, Reunion, Guadeloupe are dispatched in different datasets.

Field hierarchy and cardinality

Below is a nested list of fields likely to be used in an WMCP record, together with their cardinality.

Cardinality is denoted by [x..y]. Where the cardinality is preceded by "ISO" then the cardinality in the WMCP is the same. Where it is different, the cardinality for both ISO and WMCP is appended to the element name.

As noted in Section 8.1, many optional <<subsections>> of a WMCP record contain elements which are mandatory **only if** that subsection is used. An example of that is the .. 'identifier'/'authority'/'title', as shown on lines 53-57, in the following hierarchical list of fields (and see excerpt below), where 'identifier' is optional [0..n], and even if it is used, 'authority' is optional [0..n]; however, if 'authority' **is** used, then 'title' is mandatory [1..1].

```
53 _ ._ ._ ._ ._ .identifier_ ._ .ISO[0..n]
54_ ._ ._ ._ ._ ._ .MD_Identifier_ ._ .
55_ ._ ._ ._ ._ ._ ._ .authority_ ._ .ISO[0..1]
56_ ._ ._ ._ ._ ._ ._ ._ .CI_Citation_ ._ .
57_ ._ ._ ._ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
```

(Excerpt from ANNEX, Section 13)

The cardinality notation of [x..y] indicates the minimum and maximum allowable times that the element may be used, within that part of the hierarchy/tree.

For instance the notation:

[0..n] means that the element is optional, but can also be used any number of times;

[1..2] means that it is mandatory (there must be at least one), and may be used a maximum of two times.

```
1       MD_Metadata_ ._ .ISO[1..1]
2       _ .fileIdentifier_ .char_ ._ . WMO[1..1] , ISO[0..1]
3       _ .language_ .char_ ._ .ISO[0..1]
4       _ .characterSet_ .CODE:MD_CharacterSetCode_ ._ .ISO[0..1]
5       _ .parentIdentifier_ .char_ ._ .ISO[0..1]
6       _ .hierarchyLevel_ .char_ ._ .ISO[0..n]
7       _ .hierarchyLevelName_ .char_ ._ .ISO[0..n]
8
9       _ .contact_ ._ .ISO[1..n]
10      _ ._ .CI_ResponsibleParty
    see lines 66-99, for all fields available for CI_ResponsibleParty
11      _ ._ ._ .individualName_ .char_ ._ .ISO[0..1]
12      _ ._ ._ .organisationName_ .char_ ._ .ISO[0..1]
13      _ ._ ._ .contactInfo_ ._ .ISO[0..1]
14      _ ._ ._ ._ . CI_Contact_ ._ .
15      _ ._ ._ ._ . _ .address_ ._ .ISO[0..1]
16      _ ._ ._ ._ ._ . _ .CI_Address_ ._ .
17      _ ._ ._ ._ ._ ._ . _ .electronicMailAddress_ .char_ ._ .ISO[0..n]
18      _ ._ ._ .role_ .CODE:CI_RoleCode_ ._ .ISO[1..1]
19
20      _ .dateStamp_ .DATETIME_ ._ .ISO[1..1]
21        _ .metadataStandardName_ .char_ ._ .ISO[0..1]
22      _ .metadataStandardVersion_ .char_ ._ .ISO[0..1]
23        _ .dataSetURI_ .char_ ._ .ISO[0..1]
24
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
25      _ .spatialRepresentationInfo_ ._ .ISO[0..n]
26      _ ._ .MD_GridSpatialRepresentation
27      _ ._ ._ .numberOfDimensions_ .integer_ ._ .ISO[1..1]
28      _ ._ ._ .axisDimensionProperties_ ._ .ISO[1..1]
29      _ ._ ._ ._ .MD_Dimension_ ._ .
30
        _ ._ ._ ._ ._ .dimensionName_ .CODE:MD_DimensionNameTypeCode_ ._ .ISO[
1..1]
31      _ ._ ._ ._ ._ .dimensionSize_ .integer_ ._ .ISO[1..1]
32      _ ._ ._ ._ ._ .resolution_ .SCALE_ ._ .ISO[0..1]
33
```

```
        _ ._ ._ ._ ._ .dimensionName_ .CODE:MD_DimensionNameTypeCode_ ._ .ISO[
1..1]
34      _ ._ ._ ._ ._ .dimensionSize_ .integer_ ._ .ISO[1..1]
35      _ ._ ._ ._ ._ .resolution_ .SCALE_ ._ .ISO[0..1]
36      _ ._ ._ .cellGeometry_ .CODE:MD_CellGeometryCode_ ._ .ISO[1..1]
37      _ ._ ._ .transformationParameterAvailability_ .Boolean_ ._ .ISO[1..1]
38
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
39
40      _ .identificationInfo_ ._ .ISO[1..n]
41      _ ._ .MD_DataIdentification_ .
42
43      _ ._ ._ .citation_ ._ .ISO[1..1]
44      _ ._ ._ ._ .CI_Citation_ ._ .
45      _ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
46      _ ._ ._ ._ ._ .alternateTitle_ .char_ ._ .ISO[0..n]
47      _ ._ ._ ._ ._ .DATE_ ._ .ISO[1..n]
48      _ ._ ._ ._ ._ ._ .CI_Date_ .
49      _ ._ ._ ._ ._ ._ ._ .DATE_ .DATETIME_ ._ .ISO[1..1]
50      _ ._ ._ ._ ._ ._ ._ .dateType_ .CODE:CI_DateTypeCode_ ._ .ISO[1..1]
51      _ ._ ._ ._ ._ .edition_ .char_ ._ .ISO[0..1]
52
53      _ ._ ._ ._ ._ .identifier_ ._ .ISO[0..n]
54      _ ._ ._ ._ ._ ._ .MD_Identifier_ ._ .
55      _ ._ ._ ._ ._ ._ ._ .authority_ ._ .ISO[0..1]
56      _ ._ ._ ._ ._ ._ ._ ._ .CI_Citation_ ._ .
   see lines 43-111, for all fields available for CI_Citation
57      _ ._ ._ ._ ._ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
58      _ ._ ._ ._ ._ ._ ._ ._ ._ .alternateTitle_ .char_ ._ .ISO[0..n]
59      _ ._ ._ ._ ._ ._ ._ ._ ._ .DATE_ ._ .ISO[1..n]
60      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .CI_Date_ .
61      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .DATE_ .DATE_ ._ .ISO[1..1]
62
        _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .dateType_ .CODE:CI_DateTypeCode_ ._ .
ISO[1..1]
63      _ ._ ._ ._ ._ ._ ._ .code_ .char_ ._ .ISO[1..1]
64
65      _ ._ ._ ._ ._ .citedResponsibleParty_ ._ .ISO[0..n]
66      _ ._ ._ ._ ._ ._ .CI_ResponsibleParty_ ._ .
67      _ ._ ._ ._ ._ ._ ._ .individualName_ .char_ ._ .ISO[0..1] *C
68      _ ._ ._ ._ ._ ._ ._ .organisationName_ .char_ ._ .ISO[0..1] *C
69      _ ._ ._ ._ ._ ._ ._ .positionName_ .char_ ._ .ISO[0..1] *C
70
71      _ ._ ._ ._ ._ ._ ._ .contactInfo_ ._ .ISO[0..1]
72      _ ._ ._ ._ ._ ._ ._ ._ .CI_Contact_ ._ .
```

```
73
74      _ ._ ._ ._ ._ ._ ._ ._ .phone_ ._ .ISO[0..1]
75      _ ._ ._ ._ ._ ._ ._ ._ ._ .CI_Telephone_ ._ .
76      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .voice_ .char_ ._ .ISO[0..n]
77      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .facsimile_ .char_ ._ .ISO[0..n]
78
79      _ ._ ._ ._ ._ ._ ._ ._ ._ .address_ ._ .ISO[0..1]
80      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .CI_Address_ ._ .
81      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .deliveryPoint_ .char_ ._ .ISO[0..n]
82      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .city_ .char_ ._ .ISO[0..1]
83
        _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .administrativeArea_ .char_ ._ .ISO[0.
.1]
84      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .postalCode_ .char_ ._ .ISO[0..1]
85      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .country_ .char_ ._ .ISO[0..1]
86
        _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .electronicMailAddress_ .char_ ._ .ISO
[0..n]
87
88      _ ._ ._ ._ ._ ._ ._ ._ ._ .onlineResource_ ._ .ISO[0..1]
89      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .CI_OnlineResource_ ._ .
90      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .linkage_ .URL_ ._ .ISO[1..1]
91      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .protocol_ .char_ ._ .ISO[0..1]
92
        _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .applicationProfile_ .char_ ._ .ISO[0.
.1]
93      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .name_ .char_ ._ .ISO[0..1]
94      _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .description_ .char_ ._ .ISO[0..1]
95
        _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .function_ .CODE:CI_OnLineFunctionCode
_ ._ .ISO[0..1]
96
97      _ ._ ._ ._ ._ ._ ._ ._ ._ .hoursOfService_ .char_ ._ .ISO[0..1]
98      _ ._ ._ ._ ._ ._ ._ ._ ._ .contactInstructions_ .char_ ._ .ISO[0..1]
99      _ ._ ._ ._ ._ ._ ._ .role_ .CODE:CI_RoleCode_ [1..1].
100
101
        _ ._ ._ ._ ._ .presentationForm_ .CODE:CI_PresentationFormCode_ ._ .IS
O[0..n]
102
103     _ ._ ._ ._ ._ .series_ ._ .ISO[0..1]
104     _ ._ ._ ._ ._ ._ .CI_Series_ .
105     _ ._ ._ ._ ._ ._ ._ .name_ .char_ ._ .ISO[0..1]
106     _ ._ ._ ._ ._ ._ ._ .issueIdentification_ .char_ ._ .ISO[0..1]
107     _ ._ ._ ._ ._ ._ ._ .page_ .char_ ._ .ISO[0..1]
108     _ ._ ._ ._ ._ .otherCitationDetails_ .char_ ._ .ISO[0..1]
109     _ ._ ._ ._ ._ .collectiveTitle_ .char_ ._ .ISO[0..1]
```

```
110    _ ._ ._ ._ ._ .ISBN_ .char_ ._ .ISO[0..1]
111    _ ._ ._ ._ ._ .ISSN_ .char_ ._ .ISO[0..1]
112
113
114    _ ._ ._ .abstract_ .char_ ._ .ISO[1..1]
115    _ ._ ._ .purpose_ .char_ ._ .ISO[0..1]
116    _ ._ ._ .credit_ .char_ ._ .ISO[0..n]
117    _ ._ ._ .status_ .CODE:MD_ProgressCode_ ._ .ISO[0..n]
118
119    _ ._ ._ .pointOfContact_ ._ .ISO[0..n]
120    _ ._ ._ ._ .CI_ResponsibleParty_ ._ .
121    _ ._ ._ ._ ._ .individualName_ .char_ ._ .ISO[0..1]
122    _ ._ ._ ._ ._ .organisationName_ .char_ ._ .ISO[0..1]
123    _ ._ ._ ._ ._ .positionName_ .char_ ._ .ISO[0..1]
124    _ ._ ._ ._ ._ .contactInfo_ ._ .ISO[0..1]
125    _ ._ ._ ._ ._ ._ .CI_Contact_ ._ .
126    _ ._ ._ ._ ._ ._ ._ .phone_ ._ .ISO[0..1]
127    _ ._ ._ ._ ._ ._ ._ ._ .CI_Telephone_ ._ .
128    _ ._ ._ ._ ._ ._ ._ ._ ._ .voice_ .char_ ._ .ISO[0..1]
129    _ ._ ._ ._ ._ ._ ._ ._ ._ .facsimile_ .char_ ._ .ISO[0..1]
130    _ ._ ._ ._ ._ ._ ._ .address_ ._ .ISO[0..1]
131    _ ._ ._ ._ ._ ._ ._ ._ .CI_Address_ ._ .
132    _ ._ ._ ._ ._ ._ ._ ._ ._ .deliveryPoint_ .char_ ._ .ISO[0..1]
133    _ ._ ._ ._ ._ ._ ._ ._ ._ .electronicMailAddress_ .char_ ._ .ISO[0..1]
134    _ ._ ._ ._ ._ .role_ .CODE:CI_RoleCode_ ._ .ISO[1..1]
135
136    _ ._ ._ .resourceMaintenance_ ._ .ISO[0..n]
137    _ ._ ._ ._ .MD_MaintenanceInformation_ .
138    _ ._ ._ ._ ._ .maintenanceAndUpdateFrequency_ .
           CODE: MD_MaintenanceFrequencyCode_ ._ .ISO[1..1]
139
       _ ._ ._ ._ ._ .userDefinedMaintenanceFrequency_ .TM_PeriodDuration_ ._
 .ISO[0..1]
140    _ ._ ._ ._ ._ .updateScopeDescription_ ._ .ISO[0..n]
141    _ ._ ._ ._ ._ ._ .MD_ScopeDescription_ .
142    _ ._ ._ ._ ._ ._ ._ .dataset_ .char_ ._ .ISO[1..1]
143    _ ._ ._ ._ ._ .maintenanceNote_ .char_ ._ .ISO[0..n]
144
145    _ ._ ._ .graphicOverview_ ._ .ISO[0..n]
146    _ ._ ._ ._ .MD_BrowseGraphic_ .
147    _ ._ ._ ._ ._ .fileName_ .char_ ._ .ISO[1..1]
148    _ ._ ._ ._ ._ .fileDescription_ .char_ ._ .ISO[0..1]
149    _ ._ ._ ._ ._ .fileType_ .char_ ._ .ISO[0..1]
150
```

```
151    _ ._ ._ .descriptiveKeywords_ ._ WMO[1..n]    .ISO[0..n]
152    _ ._ ._ ._ .MD_Keywords_ .
153    _ ._ ._ ._ ._ .keyword_ .char_ ._ .ISO[1..n]
154    _ ._ ._ ._ ._ .type_ .CODE:MD_KeywordTypeCode_ ._ .ISO[0..1]
155    _ ._ ._ ._ ._ .thesaurusName_ ._ .ISO[0..1]
156    _ ._ ._ ._ ._ ._ .CI_Citation_ ._ .
   see lines 43-111, for all fields available for CI_Citation
157    _ ._ ._ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
158    _ ._ ._ ._ ._ ._ ._ .DATE_ ._ .ISO[1..1]
159    _ ._ ._ ._ ._ ._ ._ ._ .CI_Date_ ._ .
160    _ ._ ._ ._ ._ ._ ._ ._ ._ .DATE_ .DATE_ ._ .ISO[1..1]
161
       _ ._ ._ ._ ._ ._ ._ ._ ._ .dateType_ .CODE:CI_DateTypeCode_ ._ .ISO[1.
.1]
162
163    _ ._ ._ .resourceSpecificUsage_ ._ .ISO[0..n]
164    _ ._ ._ ._ .MD_Usage_ .
165    _ ._ ._ ._ ._ .specificUsage_ .char_ ._ .ISO[1..1]
166    _ ._ ._ ._ ._ .userDeterminedLimitations_ .char_ ._ .ISO[0..n]
167    _ ._ ._ ._ ._ .userContactInfo_ ._ .ISO[1..n]
168    _ ._ ._ ._ ._ ._ .CI_ResponsibleParty_ ._ .
   see lines 66-99, for all fields available for CI_ResponsibleParty
169     _ ._ ._ ._ ._ ._ ._ .individualName_ .char_ ._ .ISO[0..1]
170    _ ._ ._ ._ ._ ._ ._ .organisationName_ .char_ ._ .ISO[0..1]
171    _ ._ ._ ._ ._ ._ ._ .role_ .CODE:CI_RoleCode_ ._ .ISO[1..1]
172
173    _ ._ ._ .resourceConstraints_ ._ .ISO[0..n]
174    _ ._ ._ ._ .MD_Constraints_ . ISO[0..n]
175    _ ._ ._ ._ ._ .useLimitation_ ._ .ISO[0..n]
176    _ ._ ._ ._ .MD_LegalConstraints_ . ISO[0..n]
177    _ ._ ._ ._ ._ .useLimitation_ .char_ ._ .ISO[0..n]
178
       _ ._ ._ ._ ._ .accessConstraints_ .CODE:MD_RestrictionCode_ ._ .ISO[0.
.n]
179
       _ ._ ._ ._ ._ .accessConstraints_ .CODE:MD_RestrictionCode_ ._ .ISO[0.
.n]
180    _ ._ ._ ._ ._ .useConstraints_ .CODE:MD_RestrictionCode_ ._ .ISO[0..n]
181    _ ._ ._ ._ ._ .useConstraints_ .CODE:MD_RestrictionCode_ ._ .ISO[0..n]
182    _ ._ ._ ._ ._ .otherConstraints_ .char_ ._ .ISO[0..n]
183    _ ._ ._ ._ ._ .otherConstraints_ .char_ ._ .ISO[0..n]
184    _ ._ ._ ._ .MD_SecurityConstraints_ . ISO[0..n]
185    _ ._ ._ ._ ._ .useLimitation_ .char_ ._ .ISO[0..n]
186
       _ ._ ._ ._ ._ .classification_ .CODE:MD_ClassificationCode_ ._ .ISO[1.
.1]
```

```
187     _ ._ ._ ._ ._ .userNote_ .char_ ._ .ISO[0..1]
188     _ ._ ._ ._ ._ .classificationSystem_ .char_ ._ .ISO[0..1]
189     _ ._ ._ ._ ._ .handlingDescription_ .char_ ._ .ISO[0..1]
190
191     _ ._ ._ .aggregationInfo_ ._ .ISO[0..n]
192     _ ._ ._ ._ .MD_AggregateInformation_ .
193
194     _ ._ ._ ._ ._ .aggregateDataSetName_ ._ .ISO[0..1]
195     _ ._ ._ ._ ._ ._ .CI_Citation_ ._ .
    see lines 43-111, for all fields availablefor CI_Citation
196     _ ._ ._ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
197     _ ._ ._ ._ ._ ._ ._ .DATE_ ._ .ISO[1..1]
198     _ ._ ._ ._ ._ ._ ._ ._ .CI_Date_ ._ .
199     _ ._ ._ ._ ._ ._ ._ ._ ._ .DATE_ . DATE _ ._ .ISO[1..1]
200
        _ ._ ._ ._ ._ ._ ._ ._ ._ .dateType_ .CODE:CI_DateTypeCode_ ._ .ISO[1.
.1]
201
202     _ ._ ._ ._ ._ .aggregateDataSetIdentifier_ ._ .ISO[0..1]
203     _ ._ ._ ._ ._ ._ .MD_Identifier_ .
204     _ ._ ._ ._ ._ ._ ._ .authority_ ._ .ISO[0..1]
205     _ ._ ._ ._ ._ ._ ._ ._ .CI_Citation_ ._ .
    see lines 43-111, for all fields available for CI_Citation
206     _ ._ ._ ._ ._ ._ ._ ._ ._ .title_ .char_ ._ .ISO[1..1]
207     _ ._ ._ ._ ._ ._ ._ ._ ._ .DATE_ ._ .ISO[1..1]
208     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .CI_Date_ ._ .
209     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .DATE_ . DATE_ ._ .ISO[1..1]
210
        _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .dateType_ .CODE:CI_DateTypeCode_ ._ .
ISO[1..1]
211     _ ._ ._ ._ ._ ._ ._ .code_ .char_ ._ .ISO[1..1]
212
213
        _ ._ ._ ._ ._ .associationType_ .CODE:DS_AssociationTypeCode_ ._ .ISO[
1..1]
214
        _ ._ ._ ._ ._ .initiativeType_ .CODE:DS_InitiativeTypeCode_ ._ .ISO[0.
.1]
215
216     _ ._ ._ .spatialRepresentationType
217     _ ._ ._ ._ .MD_SpatialRepresentationTypeCode
                                                    CODE:
MD_SpatialRepresentationTypeCode  ISO[0..n]
218
219     _ ._ ._ .spatialResolution_ ._ .ISO[0..n]
220     _ ._ ._ ._ .MD_Resolution_ ._ .ISO[ ..]
221     _ ._ ._ ._ ._ .equivalentScale_ ._ .ISO[1..1]
```

```
222    _ ._ ._ ._ ._ ._ .MD_RepresentativeFraction_ .
223    _ ._ ._ ._ ._ ._ ._ .denominator_ .integer_ ._ .ISO[1..1]
224
225    _ ._ ._ .language_ .char_ ._ .ISO[1..n]
226    _ ._ ._ .characterSet_ .CODE:MD_CharacterSetCode_ ._ .ISO[0..n]
227    _ ._ ._ .topicCategory_ .CODE:MD_TopicCategoryCode_ ._ .WMO[1..n]
ISO[0..n]
228    _ ._ ._ .environmentDescription_ .char_ ._ .ISO[0..1]
229
230    _ ._ ._ .extent_ ._ .ISO[0..n]
231    _ ._ ._ ._ .EX_Extent_ .
232    _ ._ ._ ._ ._ .description_ .char_ ._ .ISO[0..1]
233    _ ._ ._ ._ ._ .geographicElement_ ._. .ISO[0..n]        (Mandatory, if
data is geospatial)
234    _ ._ ._ ._ ._ . _ . EX_GeographicBoundingBox_
235    _ ._ ._ ._ ._ . _ ._ .westBoundLongitude_ .DECIMAL_ ._ .ISO[1..1]
236    _ ._ ._ ._ ._ . _ ._ .eastBoundLongitude_ . DECIMAL_ ._ .ISO[1..1]
237    _ ._ ._ ._ ._ . _ ._ .southBoundLatitude_ . DECIMAL_ ._ .ISO[1..1]
238    _ ._ ._ ._ ._ . _ ._ .northBoundLatitude_ . DECIMAL_ ._ .ISO[1..1]
239
240
241    _ ._ ._ ._ ._ .geographicElement_ . ISO[0..n]
242    _ ._ ._ ._ ._ ._ .EX_GeographicDescription_ .
243    _ ._ ._ ._ ._ ._ ._ .extentTypeCode_ ._ .Boolean_ ._ .ISO[0..1]
244    _ ._ ._ ._ ._ ._ ._ .geographicIdentifier_ ._ .ISO[1..1]
245    _ ._ ._ ._ ._ ._ ._ ._ .MD_Identifier_ .
246    _ ._ ._ ._ ._ ._ ._ ._ ._ .code_ .char_ ._ .ISO[1..1]
247
248
249    _ ._ ._ ._ ._ .temporalElement_ ._ .ISO[0..n]
250    _ ._ ._ ._ ._ ._ .EX_TemporalExtent_ .
251    _ ._ ._ ._ ._ ._ ._ .extent_ ._ .ISO[1..1]
252
253    _ ._ ._ .supplementalInformation_ .char_ ._ .ISO[0..1]
254
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
255
256    _ .referenceSystemInfo_ ._ .ISO[0..n]
257    _ ._ .MD_ReferenceSystem_ .
258    _ ._ ._ .referenceSystemIdentifier_ ._ .ISO[0..1]
259    _ ._ ._ ._ .RS_Identifier_ .
260    _ ._ ._ ._ ._ .authority_ ._ .ISO[0..1]
261    _ ._ ._ ._ ._ .code_ .char_ ._ .ISO[1..1]
262    _ ._ ._ ._ ._ .codeSpace_ .char_ ._ .ISO[0..1]
```

```
263     _ ._ ._ ._ ._ .version_ .char_ ._ .ISO[0..1]
264
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
265
266     _ .contentInfo_ ._ .ISO[0..n]
267     _ ._ .MD_CoverageDescription_ .
268     _ ._ ._ .attributeDescription_ ._ .ISO[1..1]
269     _ ._ ._ ._ .RecordType_ ._ .
270     _ ._ ._ .contentType_ .CODE:MD_CoverageContentTypeCode_ ._ .ISO[1..1]
271
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
272
273     _ .distributionInfo_ ._ .ISO[0..1]
274     _ ._ .MD_Distribution_ .
275     _ ._ ._ .distributionFormat_ ._ .ISO[0..n]
276     _ ._ ._ ._ .MD_Format_ .
277     _ ._ ._ ._ ._ .name_ .char_ ._ .ISO[1..1]
278     _ ._ ._ ._ ._ .version_ .char_ ._ .ISO[1..1]
279     _ ._ ._ ._ ._ .amendmentNumber_ .char_ ._ .ISO[0..1]
280     _ ._ ._ ._ ._ .specification_ .char_ ._ .ISO[0..1]
281     _ ._ ._ ._ ._ .fileDecompressionTechnique_ .char_ ._ .ISO[0..1]
282
283     _ ._ ._ ._ ._ .formatDistributor_ ._ .ISO[0..n]
284     _ ._ ._ ._ ._ ._ .MD_Distributor_ .
285     _ ._ ._ ._ ._ ._ ._ .distributorContact_ ._ .ISO[1..1]
286     _ ._ ._ ._ ._ ._ ._ ._ .CI_ResponsibleParty_ .
      see lines 66-99, for all fields available for CI_ResponsibleParty
287     _ ._ ._ ._ ._ ._ ._ ._ ._ .individualName_ .char_ ._ .ISO[0..1]
288     _ ._ ._ ._ ._ ._ ._ ._ ._ .organisationName_ .char_ ._ .ISO[0..1]
289     _ ._ ._ ._ ._ ._ ._ ._ ._ .role_ .CODE:CI_RoleCode_ ._ .ISO[1..1]
290     _ ._ ._ ._ ._ ._ ._ .distributorTransferOptions_ ._ .ISO[0..n]
291     _ ._ ._ ._ ._ ._ ._ ._ .MD_DigitalTransferOptions_ .
292     _ ._ ._ ._ ._ ._ ._ ._ ._ .unitsOfDistribution_ .char_ ._ .ISO[0..1]
293     _ ._ ._ ._ ._ ._ ._ ._ ._ .transferSize_ .Real_ ._ .ISO[0..1]
294
295     _ ._ ._ ._ ._ ._ ._ ._ ._ .onLine_ ._ .ISO[0..n]
296     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .CI_OnlineResource_ .
297     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .linkage_ .URL_ ._ .ISO[1..1]
298     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .protocol_ .char_ ._ .ISO[0..1]
299     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .name_ .char_ ._ .ISO[0..1]
300     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .description_ .char_ ._ .ISO[0..1]
301     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ ._ .function_ .CODE:
CI_OnLineFunctionCode_ ._ .ISO[0..1]
302
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
303
304     _ .dataQualityInfo_ ._ .ISO[0..n]
305     _ ._ .DQ_DataQuality_ .
306     _ ._ ._ .scope_ ._ .ISO[1..1]
307     _ ._ ._ ._ .DQ_Scope_ .
308     _ ._ ._ ._ ._ .level_ .CODE:MD_ScopeCode_ ._ .ISO[1..1]
309     _ ._ ._ ._ ._ .extent_ .
310     _ ._ ._ ._ ._ .levelDescription_ ._ .ISO[0..n]
311     _ ._ ._ ._ ._ ._ .MD_ScopeDescription_ .
312     _ ._ ._ ._ ._ ._ ._ .dataset_ .char_ ._ .ISO[1..1]
313     _ ._ ._ .lineage_ ._ .ISO[0..1]
314     _ ._ ._ ._ .LI_Lineage_ .
315     _ ._ ._ ._ ._ .statement_ .char_ ._ .ISO[0..1]
316
317     _ ._ ._ ._ ._ .processStep_ ._ .ISO[0..n]
318     _ ._ ._ ._ ._ ._ .LI_ProcessStep_ .
319     _ ._ ._ ._ ._ ._ ._ .description_ .char_ ._ .ISO[1..1]
320     _ ._ ._ ._ ._ ._ ._ .rationale_ .char_ ._ .ISO[0..1]
321     _ ._ ._ ._ ._ ._ ._ .source_ ._ .ISO[0..n]
322     _ ._ ._ ._ ._ ._ ._ ._ .LI_Source_ .
323     _ ._ ._ ._ ._ ._ ._ ._ ._ .description_ .char_ ._ .ISO[0..1]
324     _ ._ ._ ._ ._ ._ ._ ._ ._ .sourceCitation_ ._ .ISO[0..1]
325     _ ._ ._ ._ ._ ._ ._ ._ ._ ._ .CI_Citation_ ._ .
326
327     _ ._ ._ ._ ._ .source_ ._ .ISO[0..n]
328     _ ._ ._ ._ ._ ._ .LI_Source_ .
329     _ ._ ._ ._ ._ ._ ._ .description_ .char_ ._ .ISO[0..1]
330
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
331
332     _ .metadataConstraints_ ._ .ISO[0..n]
333     _ ._ .MD_Constraints_ .
334     _ ._ ._ .useLimitation_ .char_ ._ .ISO[0..n]
335     _ ._ .MD_LegalConstraints_ .
336     _ ._ ._ .useLimitation_ .char_ ._ .ISO[0..n]
337     _ ._ ._ .accessConstraints_ .CODE: MD_RestrictionCode_ ._ .ISO[0..n]
338     _ ._ ._ .useConstraints_ .CODE: MD_RestrictionCode
339     _ ._ ._ .otherConstraints_ .char_ ._ .ISO[0..n]
340
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
341
342     _ .applicationSchemaInfo_ ._ .ISO[0..n]
343     _ ._ .MD_ApplicationSchemaInformation_ .
344     _ ._ ._ .name_ ._ .ISO[1..1]
```

```
345     _ ._ ._ ._ .CI_Citation_ ._ .
see lines 43-111, for all fields available for CI_Citation
346     _ ._ ._ .schemaLanguage_ .char_ .
347     _ ._ ._ .constraintLanguage_ .char_ ._ .ISO[1..1]
348
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
349
350     _ .metadataMaintenance_ .
351     _ ._ .MD_MaintenanceInformation_ ._ .ISO[0..1]
352     _ ._ ._ .maintenanceAndUpdateFrequency_ .
CODE:MD_MaintenanceFrequencyCode_ ._ .ISO[1..1]
353     _ ._ ._ .dateOfNextUpdate_ .DATE_ ._ .ISO[1..1]
354
        _ ._ ._ .userDefinedMaintenanceFrequency_ .PERIODDURATION_ ._ .ISO[0..
1]
355     _ ._ ._ .updateScope_ .CODE:MD_ScopeCode_ ._ .ISO[0..1]
356     _ ._ ._ .updateScopeDescription_ ._ .ISO[0..n]
357     _ ._ ._ ._ .MD_ScopeDescription_ ._ .ISO[0..n]
358     _ ._ ._ ._ ._ .dataset_ .char_ .
359     _ ._ ._ .maintenanceNote_ .char_ ._ .ISO[1..1]
360
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

_____

Annex 3

[The following amendment is copied from Recommends (2) and (3) of Recommendation 3.4(2)/2 (CBS-16)]

Add new Part VI to WMO-No. 1060 Manual on the WMO Information System

PART VI. INFORMATION MANAGEMENT
Note: guidance on information management best practices is provided in Part VII of the Guide to the WMO Information System (WMO-No. 1061).

PART VII OF THE GUIDE TO THE WMO INFORMATION SYSTEM

Add Part VII "Information Management" to WMO-No. 1061 Guide to the WMO Information System *and add the following as the text of that Part*

PART VI. INFORMATION MANAGEMENT
Guidance on information management best practices is provided in Part VII of the Guide to the WMO Information System (WMO-No. 1061).

[The following amendment is copied from the Annex to Recommendation 3.4(2)/2 (CBS-16)]

Add the following text in Part I of the Guide to the WMO Information System (WMO-No. 1061)

1.7.5 Guidance on the use of the direct broadcast network (DBNet) for near real-time relay of low Earth orbit satellite data is provided in the document *Guidelines to the Direct Broadcast Network (DBNet)* (WMO-No. xxxx) (http://wis.wmo.int/DBNet-Guide) that is an Attachment to this Guide.

Add the following text as Part VII of the Guide to the WMO Information System (WMO-No. 1061)

PART VII. INFORMATION MANAGEMENT

7.1 Guidance on management of information about climate reports and climate observing stations is available in the *Climate Data Management System Specifications* (WMO-No. 1131). (http://wis.wmo.int/CDMS-Specification) that is an Attachment to this Guide.

_____

Annex 4
GUIDANCE on DBNet

[The following text is copied from the Annex of Recommendation 3.4(3)/1 (CBS-16), with the addition of the text following the table of amendments that reflects Recommends (2) and (3) of that Recommendation]

WMO Information System

WMO Space Programme

GUIDE TO THE DIRECT BROADCAST NETWORK (DBNet)

For Near Real-Time Relay of Low Earth Orbit Satellite Data

WMO No. XXXX

2017

World Meteorological Organization

Weather • Climate • Water

WMO-No. xxxx

Chair, Publications Board
World Meteorological Organization (WMO)
7 bis, avenue de la Paix
P.O. Box 2300
CH-1211 Geneva 2, Switzerland

Tel.: +41 (0) 22 730 84 03
Fax: +41 (0) 22 730 80 40
E-mail: publications@wmo.int

ISBN 978-92-63-1xxxx-x

DOCUMENT REVISION TRACK RECORD

Date	*Paragraph/ Section*	*Purpose of amendment*	*Proposed by*	*Approved by*

This document is an Attachment to WMO-No. 1061 *Guide to the WMO Information System* and is designated as a technical specification.

CONTENTS

1. INTRODUCTION

1.1. PURPOSE AND SCOPE

The purpose of this Guide is to define the minimum standards applicable to the Direct Broadcast Network for Near Real-Time Relay of Low Earth Orbit Satellite Data (DBNet) and to provide guidance for implementing these standards.

In the present Guide, the verb “shall” is used when referring to the standards necessary for DBNet to work properly, and “should” when referring to recommended practices. The DBNet standards are applicable to all voluntary contributions of WMO Members to DBNet.

The aims of these standards are twofold:

- To help ensure that the data provided by each particular DBNet regional network can be used operationally to meet user requirements as recorded in the WIGOS Information Resource [RD.2];
- To facilitate inter-regional data exchange and interoperability around the globe, with a particular focus on ensuring the global consistency of the DBNet datasets.

This Guide is primarily directed to the DBNet station operators and coordinating entities. It also contains provisions for consideration by providers of processing software and by satellite operators. Furthermore, it can be a useful reference for the users of DBNet products.

1.2. STRUCTURE OF THE DOCUMENT

This Guide consists of the following sections:

Section 1: Introduction;

Section 2: Defines DBNet and describes its components;

Section 3: Addresses the overall DBNet coordination processes;

Section 4: Contains common standards and practices applicable to the production of DBNet data across all DBNet regional networks;

Section 5: Contains specific standards and practices applicable to the production of each DBNet service;

Section 6: Conclusions;

Annexes: Contain ancillary information which is provided separately for easier reference and to facilitate updating.

1.3. APPLICABLE DOCUMENTS

[AD.1]: WMO Manual on Codes, Volume 1.2, Parts B and C, WMO-No. 306
[AD.2]: WMO Manual on the GTS (WMO-No. 386)
[AD.3]: WMO Manual on the WIS (WMO-No. 1060)

1.4. REFERENCE DOCUMENTS

[RD.1]: Statements of Guidance for Global Numerical Weather Prediction and High-Resolution Numerical Weather Prediction
[RD.2]: WIGOS Information Resource, Observing System Capabilities Analysis and Review (OSCAR): www.wmo.int/oscar
[RD.3]: DBNet Network Status and Plan http://www.wmo.int/pages/prog/sat/documents/DBNet_Network-status-and-plans.pdf
[RD.4]: DBNet Coding Summary http://www.wmo.int/pages/prog/sat/documents/DBNet_Coding-summary.xls

2. OVERVIEW OF DBNet

2.1. AIM AND FUNCTIONS OF DBNet

The aim of DBNet is to provide near real-time access to near-global data from Low Earth Orbit (LEO) satellites, in order to meet in a cost-efficient manner the timeliness requirements of regional and global Numerical Weather Prediction (NWP) and other applications.

As a system, DBNet performs the following functions:

- Reception and acquisition of satellite Direct Broadcast signals at local DBNet stations;
- Processing of the acquired data into products;
- Near real-time delivery of products;
- Performance monitoring and quality control;
- User information;
- Coordination and planning.

2.2. JUSTIFICATION OF DBNet

Access to LEO data is normally relying on data dumps at one Command and Data Acquisition (CDA) station, which allows retrieving complete orbit data, however with a data latency resulting from on-board data storage between the time of acquisition and the time when the data is dumped

to the CDA. This on-board storage can be reduced roughly by a factor of two when two high-latitude CDAs are used, one in the North and the other in the South. Further reduction requires a whole network of mid- or low latitude stations distributed around the globe, which involves higher ground infrastructure costs and a highly complex scheduling of data storage and dumps.

When satellites have a Direct Broadcast capability, which is the case of most LEO meteorological satellites, an alternative data access route is the acquisition of the Direct Broadcast data stream at a local ground station, which allows real-time acquisition, albeit with coverage limited to the portion of orbit within the area of visibility of the local station.

The Direct Broadcast Network for Near Real-Time Relay of LEO satellite data (DBNet) overcomes this limitation in offering a cost-efficient trade-off between coverage and timeliness. It coordinates data acquisition through a globally distributed network of local Direct Broadcast receiving stations, their processing in accordance with agreed standards, and their rapid delivery to the global user community through appropriate telecommunication systems.

The substantial improvement in timeliness is crucial for NWP models with short cut-off, which otherwise cannot take advantage of the most recent satellite passes. This concept was initially promoted by the HIRLAM community and EUMETSAT for the collection of ATOVS data to support regional NWP over Europe. It was then extended by WMO to the global scale under the name Regional ATOVS Retransmission Services (RARS) and quickly adopted by the global NWP as the timeliness requirements of global models became more stringent. Impact studies have given evidence of the benefit of RARS for regional and global NWP. Several papers and posters on RARS are available on the WMO RARS web page (http://www.wmo.int/pages/prog/sat/rars-implementation_en.php#RARSdocs).

DBNet is expanding the RARS concept to other data types in support of a wider range of applications. The present Guide thus replaces the former RARS Operators Standards with a wider scope to accommodate new sensor data, to ensure interoperability with the NOAA Direct Broadcast Real Time Network and to take into account the WMO Information System.

2.3. DBNet COMPONENTS

DBNet is composed of several regional or sub-regional networks of receiving stations. The list of stations contributing to these networks is provided in [RD. 3].

A DBNet Network Coordinator is designated for each DBNet regional or sub-regional network.

The role of the regional/sub-regional Network Coordinators is to:

- Ensure coordination of the regional or sub-regional network, report to the DBNet Coordination Group, and contribute to the overall DBNet planning and coordination described in Section 3;
- Provide guidance to Station Operators for implementing new services, and oversee the validation procedures defined in Annex B;
- Ensure performance monitoring as defined in Section 3.2;
- Maintain a website providing information as listed in Section 3.3.

Table 1 contains the list of DBNet regional or sub-regional networks and coordinating centers.

Regional network	Regional Network Coordinator	Sub-regional network	Sub-regional Network Coordinator
DBNet-EUMETSAT (EARS European stations and other regional partners)	EUMETSAT		
DBNet-Asia-Pacific	BOM	Asia-Pacific North	JMA
		Asia-Pacific South	BoM
DBNet-South America		South America/North	INPE
		South America/South	SMN /CONAE
DBNet-NOAA (DBRTN US stations and other regional partners)(1)	NOAA/CIMSS		

(1) DBNet-NOAA is implemented by NOAA/CIMSS in partnership with EUMETSAT and shares some functions with EARS.

Table 1: DBNet regional or sub-regional network components

Global Monitoring Centres should perform a systematic control of product consistency. This function is assumed by the EUMETSAT NWP SAF, led by the Met Office (United Kingdom) for the IR/MW sounding service. For other services global monitoring centres have not yet been identified.

The list of Network Coordinators is maintained by the WMO Secretariat and is available online as Operational Information. (Currently: http://www.wmo.int/pages/prog/sat/dbnet-implementation_en.php#DBNetcontacts).

Each DBNet regional or sub-regional network contributes to one or several DBNet "Services". A DBNet Service is performing the acquisition and relay of a certain category of satellite data. Table 2 lists the DBNet services (current and potential).

Categories of Services	Services (Instruments)
IR/MW sounding	RARS (AMSU-A, MHS, HIRS), ATMS, VASS (MWTS/2, MWHS/2, IRAS)
IR/VIS imaging	VIIRS, AVHRR, MERSI
Hyperspectral IR sounding	CrIS, IASI, HIRAS, AIRS
Scatterometry	ASCAT, Wind RAD
MW imagery	MWRI

Table 2: Current and potential DBNet services (as of August 2016)

Significant NWP user interest has been expressed for data from the Russian MW imaging/sounding radiometer MTVZA-GY, manifested on the METEOR series of satellites. The feasibility of including this instrument in the DBNet services will be further analysed.

A service based on GNSS Radio-occultation data could be considered for DBNet, as the Metop satellites and the FY-3 satellites fly GNSS-RO instruments. Due the limb-sounding nature of the GNSS-RO such a service would not produce regional atmospheric profiles, but for space weather application there is an interest in fast delivery of global data from the ionosphere. The feasibility of such a service requires further analysis, which will be undertaken together with CGMS.

2.4. HIGH-LEVEL SERVICE SPECIFICATIONS

The DBNet Service Specifications are determined with the aim to respond to user requirements of WMO Application Areas, as recorded in OSCAR [RD.2]. For example, the requirements of Global NWP (http://www.wmo-sat.info/oscar/applicationareas/view/1) and High-Resolution NWP (http://www.wmo-sat.info/oscar/applicationareas/view/2) require for atmospheric temperature, humidity profiles and wind vector at sea surface, a timeliness of less than 6 to 15 min as a goal and 30 min as breakthrough. The DBNet specifications represent the agreed commitment by DBNet Regional Networks to contribute to meeting these requirements, taking into account the technical capabilities and resource constraints. The table below summarizes the operational service specification for each DBNet Service category.

These specs will be validated in consultation with relevant user groups, for example the GODEX-NWP as representing the global NWP data exchange community and the ITWG representing the satellite atmospheric sounding community.

The DBNet high-level specifications are summarized in Table 3.

Category of Service	Driving Application	Products	Data latency goal/threshold	Availability	Coverage
IR/MW sounding	Global and High-Resolution NWP	Level 1 brightness temperatures	20 min/ 30 min	95%	90%
IR/VIS imaging	Nowcasting	Level 1 radiance /reflectivity	10 min/ 20 min	95%	30%
HiRes IR sounding	Global and High-Resolution NWP	Level 1 radiances and PC scores	20 min/ 30 min	95%	90% (60% initially)
Scatterometry	NWP, Nowcasting and Ocean Applications	backscatter cross-sections	20 min/ 30 min	95%	50% (of oceanic areas)
MW imagery	NWP, Nowcasting,	Level 1 brightness temperatures	20 min/ 30 min	95%	30%

Table 3: DBNet High-Level Service Specifications

Data latency is defined here as the maximum time elapsed between observation time (sensor time) and the availability on the WMO Information System (WIS) core network to be satisfied by at least 90% of the data.

The availability rate is an indicator of the target uptime for a DBNet station when there is no special operational constraint (i.e. not considering particularly remote sites such as Antarctic stations). It is defined here as the percentage of days where the station is operating normally. The number of passes acquired depends on local factors (including the station latitude and the scheduling priorities) and cannot be fixed as a high-level specification, but is monitored (e.g. on a monthly basis) as a performance indicator. The availability is defined for an individual station. Adjacent stations with significantly overlapping acquisition areas can back-up each other, which is important primarily to solve possible reception scheduling conflicts.

The coverage is defined here as the percentage of the Earth's surface that can be viewed by the relevant satellite instrument and the data transmitted to DBNet stations via direct broadcast. This is calculated in merging the areas of visibility of the local stations contributing to the service. As an order of magnitude, an isolated station (not overlapping with the area of visibility of another station) without mask contributes to the global coverage by about 4%. (Note: this index takes only into account the latitudes between 82°S and 82°N which are flown over by sun-synchronous satellites.)

3. DBNet COORDINATION

3.1. DBNet NETWORK IMPLEMENTATION

The WMO Secretariat and all DBNet Network Coordinators strive to ensure smooth operation of the DBNet Services across all regional networks, to plan expansion of DBNet, to review the priorities and to take any appropriate measure to meet evolving user requirements. The regional/sub-regional Network Coordinators identify candidate stations and negotiate agreements with Station Operators with a view to expand the network and fill gaps when necessary.

This coordination is achieved through the DBNet Coordination Group, the Terms of Reference of which are provided in Annex A.

The WMO Secretariat maintains a list of DBNet contributing stations associated to each regional network with the status and plans of the different services [AD.4], based on the reports from DBNet Network Coordinators. This allows monitoring the coverage of the respective DBNet services.

The procedure contained in Annex B describes the steps to be followed for adding a station to DBNet, modifying its status, or removing it from DBNet.

3.2. QUALITY OF SERVICE

3.2.1. Quality assurance

In order to help ensure that the service provided is of an appropriate quality, the DBNet Station Operator shall:

- Uutilize an appropriate system for the tracking and resolution of operational anomalies;
- Ensure that all operations and maintenance staff are appropriately trained;
- Ensure that appropriate provisions are in place to protect against unauthorized access to the DBNet equipment (from both physical, and network security points of view);
- Ensure that the maintenance approach (e.g. levels of redundancy, spares holdings, maintenance contracts and maintenance team size) is consistent with the service availability targets (see section 2.4);
- Ensure that adequate arrangements are in place to monitor the satisfactory performance of the service (supported by the availability of validated operational and maintenance procedures.

3.2.2. Quality control

Each DBNet Regional Network shall implement appropriate quality control measures to monitor the integrity of DBNet data that are disseminated, in particular with respect to timeliness and correct formatting.

The regional/subregional Network Coordinators:

- Organize the near real-time monitoring function;
- Maintain the list of operational points of contacts of individual station operators;
- Perform overall performance monitoring (including implementation of the standards);
- Manage software updates to ensure that proper software versions are used on each station;
- Ensure an operational point of contact for resolving anomalies.

For the IR/MW sounding and Hyperspectral IR sounding services, global monitoring is performed by the EUMETSAT NWP SAF to assess the consistency of DBNet data with the global data and their timeliness. The results of this monitoring are sent to the operators and statistics are published online, see NWP SAF website http://nwpsaf.eu.

3.2.3. Issue management

Each DBNet Station operator and each DBNet Network Coordinator shall designate an Operational Point of Contact to be contacted in case of operational problems.

The contact details of Operational Points of Contact of each regional/sub-regional network will be posted on the DBNet Regional Network website to allow the users to report operational problems. Depending on the nature of the problem, the DBNet coordinating entity will contact the relevant DBNet station operator, the relevant WIS DCPC/GISC as defined in Appendix B of [AD.3], and/or the global monitoring unit (EUMETSAT NWP SAF Help Desk).

Each DBNet Network Coordinator should implement appropriate issue management processes in order to properly track and manage the resolution of problems, including notification of the providers of pre-processing software packages.

Each DBNet Processing Software Provider of a pre-processing software package should implement software anomaly management processes, for fast resolution of software problems that affect the end-users.

3.3. PUBLICATION OF SERVICE INFORMATION

The WMO Space Programme provides and maintain a DBNet e-mail list-server, which allows DBNet Network Coordinators and Processing Software Providers to support all Station Operators and operational Users by keeping them up-to-date with system changes (e.g. announcement of AAPP and CSPP S/W releases and their impact on DBNet operations).

Each DBNet regional or sub-regional Network Coordinator should also maintain a website containing an up-to-date description of the service, including:

- For each Service, the instruments and satellites from which data are collected;
- The geographic coordinates of the collection stations that form part of the DBNet data collection network, together with the associated geographical coverage maps;
- The processing software versions that are used to generate the products for the stations in the regional network;
- The target timeliness and target availability of the service;
- Details of the data distribution mechanism and any associated user reception equipment requirements (e.g., for receiving data from a satellite direct broadcast system);
- File naming and structure;
- The administrative procedures to be followed by a user to gain access to the data;
- A link to the scheduling priorities (including any instrument/satellite priorities);
- Operational points of contact of the Network Coordinator allowing users to report problems with the service (including generic e-mail addresses).

When this information is available for individual stations:

- Planned acquisition schedule;
- Acquired passes in the last 24 hour period compared to the planned acquisition schedule (referenced to the planned acquisition schedule);
- Long-term planning information that may affect the service in the future (e.g., planned outages, upgrade of software version, etc.);
- Quality monitoring results.

Each DBNet Processing Software Provider maintains on its website a record of the current recommended software versions and configurations.

For operational issues strictly related to the distribution of DBNet products through the WIS core networks (including e.g. RMDCN), WIS communication procedures must be followed.

4. COMMON DBNet STANDARDS AND RECOMMENDED PRACTICES

4.1. INTRODUCTION

The common standards and recommended practices cover aspects of DBNet operations that are not specific to a particular service and should apply for any regional network contributing to the overall DBNet network. The standards are mandatory and are only defined in areas that affect the interoperability of DBNet regional networks, the access to and the utilization of DBNet products, and the interface to the WIS. On the other aspects, some practices are recommended or indicated as guidance, but the actual implementation can be defined in an optimal manner by each DBNet regional network.

A DBNet Network Coordinator is defined as the managing entity responsible for ensuring an end-to-end service within a particular region (i.e., with responsibility for data collection from the HRPT stations, processing, dissemination of the products to users and inter-regional data exchange). If responsibility for the implementation of these functions is shared between several parties, then it is the responsibility of the lead entity to ensure that all the involved parties comply with the relevant parts of this standard.

Overall DBNet standards and recommended practices are defined in the following areas:

- Product processing and product format;
- Product registration and distribution;
- Quality of service;
- Operations and maintenance including anomaly processing;
- Publication of service Information;
- DBNet network coordination.

4.2. ACQUISITION

4.2.1. Satellite acquisition scheduling priorities

Guidelines for satellite acquisition scheduling priorities are established by the DBNet Coordination Group considering:

- Availability and timeliness of global data;
- Equatorial Crossing Time diversity;
- Instrument health;
- DB signal quality;
- Ability of NWP to assimilate instruments.

The scheduling priorities are reviewed annually or when needed. The current priorities are recorded in an Operational Information maintained on the WMO Space Programme website (www.wmo.int/pages/prog/sat). As an example, the 2015 priorities are listed in Annex C.

4.3. PRODUCT PROCESSING (COMMON ASPECTS)

4.3.1. Processing Level

Any products exchanged inter-regionally shall be at level 1, unless otherwise specified for the specific service.

Level 1 is understood to be radiances, reflectances or brightness temperatures for sounders and imagers and sigma-0 or kp for scatterometers, all on original instrument grid with geolocation data.

The AAPP Software Description (http://nwpsaf.eu/site/software/aapp/documentation/) includes the following definition of processing levels:

“Level 0: HRPT data (NOAA) or PFS L0 (METOP): Raw telemetry data including housekeeping and others raw data. Data of the different instruments are merged into a HRPT stream for NOAA. One file per instrument for METOP.

AAPP level 1a: separated data for each instrument AAPP level 1b: Earth located and calibration coefficients (reversible: calibration coefficients are separated from raw data).
AAPP level 1c: Earth located and converted to brightness temperature data (non-reversible: calibration coefficients are applied to data) AAPP level 1d: Mapped and filtered data (with optional cloud mask in the case of HIRS).
PFS level 1B (for AVHRR): Earth located and calibration coefficients, flags.
PFS level 1C (for IASI): Gaussian-apodised, resampled radiance spectra, corrected for all geometrical and instrumental effects, with mapped AVHRR. Earth located.

For SNPP, JPSS and some other programmes (e.g. DMSP), NOAA have adopted the following naming convention, and these names are used in the AAPP documentation where applicable:

- Raw data records (RDR): Raw data from the instrument.
- Temperature data records (TDR): Calibrated, geolocated antenna temperatures from microwave sounder (i.e. no correction for antenna pattern). Original instrument grid.
- Sensor data records (SDR): Calibrated, geolocated brightness temperatures, radiances or reflectivities. In the case of microwave instruments, antenna correction has been applied. Either original instrument grid or re-mapped.
- Environmental data records (EDR): Geophysical quantities.”

Processing to level 1, and BUFR encoding, can be done at the regional centre, or locally at the receiving station location.

The DBNet Network Coordinator is responsible for ensuring that appropriate local centre and sub-centre codes are defined and are included in the BUFR messages as described in Section 4.4.

4.3.2. Product Processing Packages

DBNet Network Coordinators and Stations Operators shall use agreed processing packages and agreed auxiliary input data such as orbit information and instrument calibration files in order to ensure that the processed products are fully consistent with the corresponding global data sets pre-processed by the respective satellite operators.

The suite of processing packages to be used by DBNet is described below and is detailed in the sections of this document addressing specific services. The list of software processing packages and organizations responsible for maintaining them is provided in the following tables. For the

scatterometry and MW imagery services, information about processing packages will be included when they become generally available.

Level-0 Processing Packages			
Package	Satellites	Provider	Comment
RT-STPS	SNPP, Metop, FY-3, Aqua	NASA DRL	CADU to CCSDS Source Packets
FY3L0PP	FY-3	CMA	CADU to CCSDS Source Packets
Metopizer	Metop	EUMETSAT	CCSDS Source Packets to EPS Level-0

Table 4: Level-0 Processing Packages

Level-1 Processing Packages			
Package	DBNet Service	Provider	Comment
AAPP	RARS, AVHRR	EUMETSAT (via NWP SAF)	
OPS-LRS	IASI	EUMETSAT (via NWP SAF)	Released as an optional part of AAPP.
CSPP	ATMS, CrIS, VIIRS	NOAA (via SSEC, UW-Madison)	
FY3L1PP	VASS, MERSI	CMA	
IMAPP	AIRS, Aqua AMSU	SSEC, UW-Madison	

Table 5: Level-1 Processing Packages

Encoding Packages			
Package	DBNet Service	Provider	Comment
AAPP	RARS, IASI, ATMS, CrIS, VASS	EUMETSAT (via NWP SAF)	Requires BUFR library
IMAPP	AIRS, Aqua AMSU	SSEC, UW-Madison	
CVIIRS	VIIRS	EUMETSAT	Converts between VIIRS SDR and Compact VIIRS SDR

Table 6: Encoding Packages

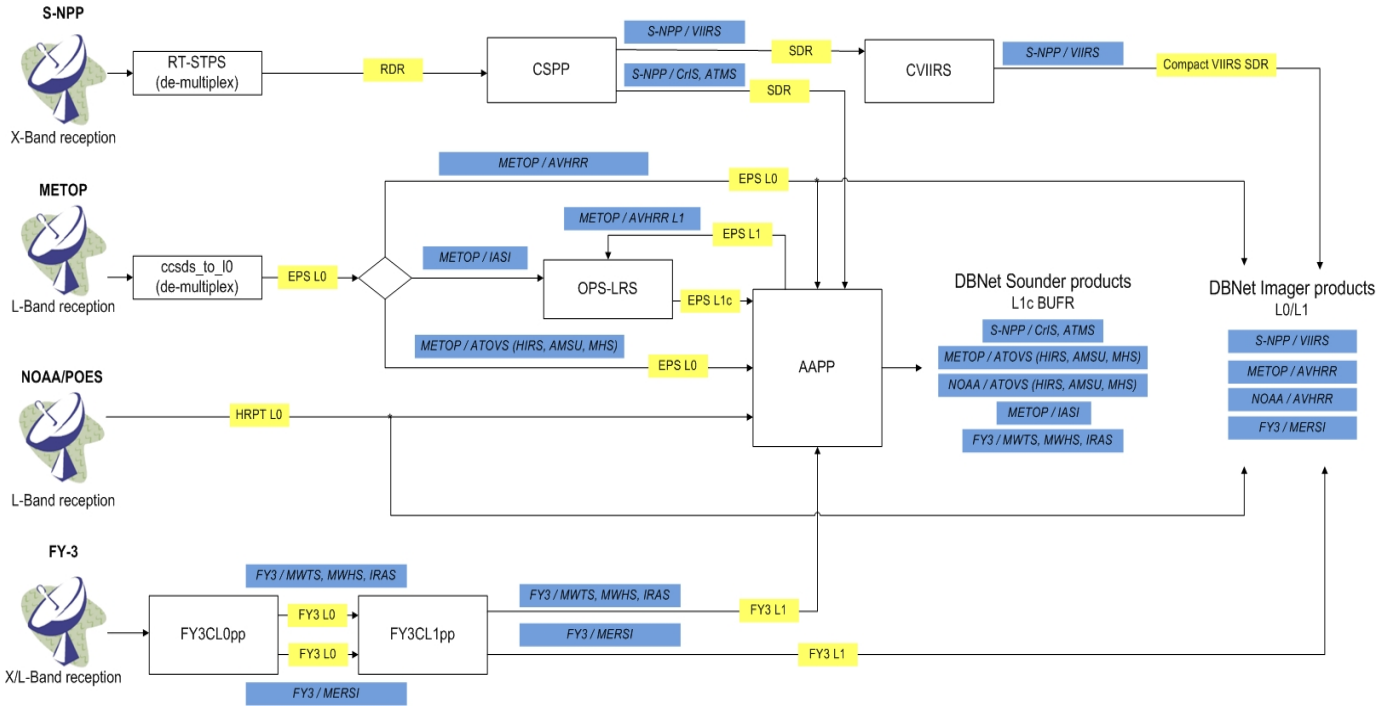


Figure 1: Schematic diagram of processing packages to be used for DBNet

4.3.3. Auxiliary Data

A Direct Broadcast station requires satellite orbit information in the form of Two Line Elements (TLE) for the prediction of future satellite passes, for antenna pointing during the acquisition of satellite data and for processing and geolocation of the sensor data. Orbital elements shall be updated at least once per day.

Additional instrument processing related auxiliary data are also required.

- For AAPP, auxiliary data files are provided by the NWP SAF (www.nwpsaf.eu).
- For CSPP, auxiliary data files for processing of VIIRS, CrIS, and ATMS are obtained periodically from NOAA operations and are made available for Internet download by the CSPP team. This includes TLEs and PolarWander files, as well as Calibration Tables. DBNet operators are encouraged to run the automated lookup table update scripts supplied with the CSPP SDR software regularly to ensure the most up to date auxiliary data are available.

Currently (August 2016) orbital data are made available directly by satellite operators at:

- Metop: http://oiswww.eumetsat.org/metopTLEs/html/index.htm (“long TLEs”) or the Multi-Mission Administration Messages contained in the Metop HKTM L0 files.
- NOAA: https://www.space-track.org (login needed) or http://celestrak.com/NORAD/elements/.
- FY3: http://www.shinetek.com.cn/eos_data/ or http://satellite.cma.gov.cn/portalsite/default.aspx.

For the future it is planned that each satellite operator will make TLE data publicly available in a standardized manner, along the lines of the service provided by NOAA for the SNPP satellite under https://msds.npoess.noaa.gov/MSDS/AUXILIARY/tle/. This will enable station operators, in an automated manner, to select the most recent reference TLE date and time in order to propagate

the orbit into the future in the most accurate way, taking into account in particular spacecraft manoeuvres. Such procedure will be further detailed and submitted to CGMS satellite operators for endorsement as a technical standard. The following description is a preliminary overview only.

- TLE files are made publicly available on the Internet based on the HTTPS protocol. The files are standard ASCII text files each containing a single set of TLE data in the well-established two-line format, see for example https://www.space-track.org/documentation#/tle.

- As indicated in Table 7, the file name starts with the satellite name and the reference date and time (starting with "r") of the TLE. The reference date and time are defined by the satellite operator and indicate the time of the orbit determination campaign which the TLE is based on.

- The newer generations of polar orbiting satellites typically perform manoeuvres as part of routine orbit maintenance. To account for this the TLE filename should systematically include the TLE interval of validity. The interval is defined by the dates and times of the start (starting with "s") and end (starting with "e") of the validity, where the start and end are defined by the satellite manoeuvre execution times.

- If the start of validity is left undefined (all zeros), the TLE is valid until a manoeuvre as shown in the first example in Table 7. If both start and end are defined, the TLE is valid between two manoeuvres as shown in the second example in Table 7. If the end is left undefined, the TLE is valid after a manoeuvre a shown in the third example in Table 7. This scheme supports both the issuing of predicted post-manoeuvre TLEs and the issuing of determined post-manoeuvre TLEs.

- Finally, both the start and end of the validity interval can be left undefined as shown in the fourth example in Table 7. This indicates that the satellite is either not performing manoeuvres (example NOAA POES) or that there are no recent or planned manoeuvres for the satellite.

TLE Filename	Explanation
Metop-B_r20150820120000Z_s00000000000000Z_e20150823123000Z.txt	Issued on 20 August 2015. Validity ending on 23 August 2015 at 12:30 UTC (first manoeuvre).
Metop-B_r20150820120000Z_s20150823123000Z_e20150823141100Z.txt	Issued on 20 August 2015. Validity starting on 23 August 2015 at 12:30 UTC (first manoeuvre) and ending on 23 August 2015 at 14:11 UTC (second manoeuvre).
Metop-B_r20150824020000Z_s20150823141100Z_e00000000000000Z.txt	Issued on 24 August 2015. Validity starting on 23 August 2015 at 14:11 UTC (second manoeuvre).
Metop-B_r20151005120000Z_s00000000000000Z_e00000000000000Z.txt	Issued on 5 October 2015. No validity limitations.

Table 7: Example of TLE filenames for semi-open, closed and open intervals of validity.

4.3.4. Segmentation

Classically the raw satellite data acquired by a Direct Broadcast reception station is transferred to the product processing system after completion of the full satellite pass.

To achieve the challenging DBNet timeliness requirements, it can however be necessary for certain services (e.g. IR/VIS imagery) to transfer the data in segments, shorter than the full satellite pass, during the pass. Each segment is transferred to the product processing system as soon as its acquisition is completed. The duration of a segment is a configurable parameter, typically set to 2 minutes. The last segment of a pass may be shorter to match the overall duration of the pass.

It is recommended to transfer the data as CCSDS CADU, CCSDS VCDU or CCSDS Source Packets without adding any additional structure to the data and with each segment containing a sequence of complete CCSDS packets. These formats are well defined and enable easy segmentation and concatenation. CCSDS CADU is recommended as the most generic. CCSDS VCDU or CCSDS Source Packets can be chosen if data from a subset of instruments is required and the overall bandwidth of the transfer is of concern.

A typical implementation is based on the FTP protocol with the reception station acting as the FTP client and the product processing system as the FTP server. To improve the reliability of the transfer in the presence of equipment resets on either side or short interruptions of the network, the FTP client shall implement a retry mechanism. An appropriate mechanism could be for example to retry up to 10 times with a time interval between retries of 30 seconds.

The segment file name should indicate the name of the satellite, start of pass date, start of pass time, segment start time, segment end time, orbit number and station acronym. To simplify the handling of the segments by the product processing system, it is recommended that the last segment of a pass additionally has an indication that it is the last segment, that segments are transferred in order of acquisition and that during an ongoing FTP transfer the filename has an indication that the file is temporary and incomplete, e.g. by adding a suffix of .temp and atomically renaming the file once its transfer is complete.

Further details can be found in the service-specific paragraphs below.

The data acquisition and processing architecture can further be optimized in order to eliminate duplication of data. A possible approach is the one used by the EARS pilot AVHRR service, employing line-by-line acquisition planning to ensure no overlaps between neighbouring stations. The issue of overlap will be addressed in future revisions of the guide.

4.3.5. Global and local product consistency

Global (full orbit central processing) and local (usually direct broadcast) product consistency specifications are set based on considerations of NWP requirements.

Global and local product processing shall be harmonized in that brightness temperature products derived from both paths agree within tolerances that are not greater than few tenths (goal is 10%) of the respective performance requirements for bias error at a reference brightness temperature.

As a concrete example, this implies that for the MWS instrument to be flown on Metop-SG, the relevant performance requirement is the bias variation over an orbit (0.2K) – because DBNet

products will be used regionally to complement global data. So the goal for local-global consistency should be 10% × 0.2K = 0.02K.

The instrument navigation shall be harmonized in that geographical coordinates derived from both paths agree within 10% of nadir Instantaneous Field of View (IFOV) for sounder instruments and 50% of nadir IFOV for imagers. Current recommended values are displayed in the NWP SAF monitoring plots for DBNet products.

4.4. PRODUCT CODING AND FORMAT (COMMON ASPECTS)

4.4.1. Format harmonization: general principles

In order to ensure that all DBNet products are fully interoperable, it is important that all DBNet operators use WMO standard formats, with the same implementation of these formats, and follow the agreed DBNet conventions in the implementation of these formats. For instance, for BUFR the same globally defined BUFR Table D sequence descriptors (also known as templates see [AD.1]) shall be used. These templates are embedded within the BUFR tables, which along with the conversion software will be released together with the recommended service specific processing software. All DBNet Operators shall make use of this recommended, or equivalent, BUFR conversion software for format conversion.

A “DBNet product” is the result of the processing of the data acquired by one station, from one satellite pass, from one instrument. A DBNet product shall be comprised of a series of BUFR encoded messages, which shall each be included in a bulletin, which should all preferably be embedded in one file. DBNet formatting standards are thus defined at three different levels: BUFR message; Meteorological Bulletin; Filenames.

- The first level of standardization of DBNet product format is the BUFR Message encoding. For each satellite pass and each instrument (with the exception of imagery products), DBNet products are encoded in BUFR messages. Because of GTS message size limitations, a DBNet product exchanged on the GTS must be segmented into several BUFR messages. The number of BUFR messages needed for one product depends on the instrument and the duration of the satellite pass. The BUFR Message encoding should be in accordance with the Manual on Codes [AD.1] with DBNet specific provisions for Section 1 (Identification) and Section 3 (Data Description) of the BUFR message as described in Section 4.4.2.

- The second level of standardization of DBNet product format is the Abbreviated Bulletin Heading. An Abbreviated Heading is assigned to each BUFR message to form a “Meteorological Bulletin”. The bulletin heading information is used by Regional Telecommunication Hubs (RTHs) to organize the routing of the messages over the GTS. The bulletin heading is not generally used by users of the BUFR messages to interpret the information; as all the necessary information to decode the BUFR message is contained within the actual BUFR message (in combination with the associated Code Tables - see the WMO Manual on Codes). Hence there is some duplication of information between Section 1 of the BUFR message and the bulletin headings (albeit with different representations). The structure of the heading is described in “Explanation of Data Designators $T_1T_2A_1A_2$ii CCCC YYGGgg BBB ([AD.2], Vol I, Part II, 2.3.2.2/Attachment II-5)”. The different Bulletins composing a product have all the same headings, with the exception of the number “ii” which differentiates the individual Bulletins of the same product. Specific provisions are defined in Section 4.4.3 for the determination of $T_1T_2A_1A_2$ in the case of DBNet products.

As the WIS continues to evolve, and the focus progressively shifts from bulletins to files, it is anticipated that this issue will assume less relevance. However, for the time being, bulletins remain a much-used communication mechanism within the WIS, and harmonization of bulletin headings is required within the DBNet network;

- The third level of standardization of DBNet products is the file. DBNet production centres can submit products to the GTS either directly as Meteorological Bulletins, or embedded in files. These files shall follow the WIS file naming convention: pflag_productidentifier_oflag_originator_yyyyMMddhhmmss[_freeformat].type[.compression]. Guidance for DBNet product filenames are provided in Section 4.4.4.

  [Note: More explanations on "Accumulating messages into files can be found in the Manual on the GTS [AD.2] Vol.1, Part II, Attachment II-15, as of page 158].

The DBNet conventions applicable to the BUFR identification section, the BUFR data description, the abbreviated heading and the file name are summarized in the DBNet Coding Summary [RD.4], which is posted on the DBNet website: http://www.wmo.int/pages/prog/sat/documents/RARS_Coding-summary.xls .

[Note: the template will be reviewed in order to accommodate the additional DBNet Services]

4.4.2. Encoding of the DBNet BUFR Message

The structure of the BUFR Message is defined in the Manual on Codes [AD.1]. In order to facilitate identification and use of BUFR messages containing DBNet products, a specific convention shall be followed to determine certain fields of the identification section (Section 1) and for the data description section (Section 3).

The BUFR tables and Common Code Tables (CCT) referred to in this section are extracted from the Manual on Codes, Vol. I.2 [AD.1] and can be found at: https://www.wmo.int/pages/prog/www/WMOCodes/WMO306_vI2/LatestVERSION/LatestVERSION.html

Section 1, Octets 5-6: Identification of Originating/Generating Centre

The Originating/Generating Centre shall indicate the centre responsible for the processing to level 1 and BUFR encoding.

If processing to level 1 and BUFR encoding are done locally at the station site, then the Originating/Generating Centre is the organization responsible for the station. If the processing to level 1 and/or the BUFR format conversion are performed, or managed by the DBNet regional centre, then the Originating/Generating Centre is the DBNet Regional Centre.

The corresponding ID is defined in Common Code Table (CCT) C-11 and recalled in [RD.4]

Section 1, Octets 7-8: Identification of Originating/Generating Sub-centre

The Originating/Generating Sub-centre shall indicate the Direct Broadcast station that receives the data. Each sub-centre is defined with reference to the Originating/Generating Centre it is functionally related to for the considered application.

The corresponding ID is defined in CCT C-12 and recalled in [RD.4].

The sub-centres ID are allocated by the relevant centres and shall be shared with the WMO Secretariat for inclusion in CCT C-12 and [RD.4]

Section 1, Octet 11: International Data Category

The data category indicated in Octet 11 is defined by BUFR Code Table A which gives e.g. “3” for satellite vertical sounding data, “12” for satellite surface data, “21” for satellite radiance data, “24” for scatterometry, and “101” for satellite image data. (See Annex D)

Section 1, Octet 12: International Data Sub-category

Subcategories of the above categories are defined by CCT C-13 for specific instruments (AMSU-A, AMSU-B, HIRS, MHS, IASI, SSMI, ASCAT, CrIS, ATMS, VIIRS) or for generic types of instruments (IR sounding, Hyperspectral sounding, MW sounding, radio-occultation).

Octet 12 of section 1 (BUFR Edition 4) must be populated using an appropriate International sub-category. When an instrument specific entry exists in CCT C-13, this should be used. If there is no specific entry in CCT C-13 for the instrument, the most appropriate generic instrument category entry should be used. If no generic entry in CCT C-13 is applicable, a request should be made to have such an appropriate entry added to the table.

Additional details can be provided in Octet 13, which is available to indicate a local sub-category (e.g. to differentiate instruments of the same sub-category, or different operating modes of an instrument, see Annexes D and E).

Section 3: The Data Description section (Section 3) includes a definition of the elements that are used to build the message. This definition usually takes the form of a single Table D sequence descriptor. It is recommended that WMO-approved sequences are used, as given in the following table.

Instrument	Sequence (F-X-Y)	Comment
HIRS	3-10-008	20 channels
AMSU-A	3-10-009	15 channels
MHS	3-10-010	5 channels
IASI	3-40-008	Channels + PCs (variable)
CrIS	3-10-060	Channels (variable)
ATMS	3-10-061	22 channels
MWTS-2	TBD	
MWHS-2	TBD	
IRAS	TBD	

Table 8: Section 3 data descriptor sequences

If an agreed Table D sequence is not available (the case for FY-3 instruments as of August 2016), then a list of Table B descriptors may be used.

Consistency with the equivalent global data should be maintained. Usually the agency responsible for dissemination of the global data is responsible for defining the BUFR sequence.

4.4.3. Bulletin Headings

The structure of the abbreviated bulletin heading is: **$T_1T_2A_1A_2$iiCCCCYYGGgg(BBB)** as described in [AD.2] “Explanation of Data Designators $T_1T_2A_1A_2$ii CCCC YYGGgg BBB (Manual on the GTS, Vol I, Part II, 2.3.2.2/Attachment II-5)”.

For DBNet products, the following implementation shall be applied:

- **T_1T_2** should be set to “IN”;
- **A_1** identifies the instrument (i.e. A=AMSU-A, B=AMSU-B, H=HIRS, M=MHS…..). Harmonization of instrument identifiers in the bulletin heading and the filename is desirable (i.e. the value of A_1 in the bulletin heading and the <data designator> value in the filename should be harmonised). (See Annex E)
- **A_2** is the geographic area designator - as per Table C3 of the Manual on the GTS (see https://www.wmo.int/pages/prog/www/ois/Operational_Information/Publications/WMO_386/AHLsymbols/TableC3.html). Concerning the value of A_2, a Regional Indicator or a Global Indicator (“X”) can be used, depending on the most appropriate characterisation of the coverage. Where meaningful, the use of regional indicators is encouraged (e.g. “N” for Arctic and “S” for Antarctic stations).

Examples:

Bulletin headings from Casey:

INAS01 AMMC YYGGgg (for AMSU-A data)
INBS01 AMMC YYGGgg (for AMSU-B data)
INHS01 AMMC YYGGgg (for HIRS data)

4.4.4. Filenames

i) DBNet data files shall follow the GTS file-naming convention (with pflag=W) (see [AD.2]);

ii) A metadata file (which would generally be static) shall be associated with each DBNet data file.

The filename structure should be of the form:

W_productidentifier_oflag_originator_yyyyMMddhhmmss[_freeformat].type[.compression]

Where:

productidentifier is a variable length field that describes the nature of the data in the file. It consists of 2 parts; a “static part” and an “optional part” – which is not used in the context of DBNet.

The **“static part”** is the product description and consists of**:**

<**location indicator**>, <**data designator**>, <**free description**>

Where <**location indicator**> defines the producer: Country, Organization and the Production Centre. For example: for Brazil <**location indicator**> could be “br-INPE-cp”

Where <**data designator**> specifies the type of data with reference to the categories and sub-categories defined in the Common Table C-13 of the Manual on Codes, with “+” used to indicate composite data.

In the context of DBNet the following convention is used:

<**data designator**> should be the instrument name without a separator, for example: amsua, amsub, hirs, mhs, iasi or ascat (See Annex F).

<**free description**> should be used to indicate satellite and originating HRPT station, and should be preceded by “DBNet”. For example: for data from NOAA-17 from Cachoeira Paulista the <free description> should read “DBNet+noaa17+cpt”. Note: For backward compatibility “rars” can be used instead of “DBNet”.

(See details in Annex F.)

oflag – at this time the only admissible value of **oflag** is “C” – indicating that the <originator> field will be decoded as a standard CCCC country code (and the use of the CCCC value in filenames and bulletins should be consistent).

originator is a variable length field indicating where the file originated from (and is decoded according to the value of <oflag>). For example: “SBBR” for Brasilia Airport.

yyyyMMddhhmmss is a fixed length date and time stamp field, containing the **time of BUFR file creation.**

[_freeformat] in the context of DBNet should be “_(AAPP filename)_bufr”. This usage needs to be shared with users of DBNet data.

type in the context of DBNet this value would typically be set to “bin” to indicate file containing data encoded in a WMO binary code form such as BUFR.

So a typical filename for AMSU-A data from NOAA17 provided by CPTEC/INPE in Brazil, from the HRPT station in Cachoeira Paulista, could be:

W_br-INPE-CP,amsua,DBNet+noaa17+cpt_C_SBBR_20110701090858_(AAPP filename)_bufr.bin

4.5. DBNet PRODUCTS REGISTRATION AND DISCOVERY

4.5.1. WIS discovery metadata

In order to make the DBNet products discoverable in the WMO Information System they shall be registered in the WIS discovery metadata catalogue with a metadata entry (Manual on WIS [AD.3] Appendix C). This enables any WMO Member to be aware of the availability of these products through the WIS catalogue and, if interested, to request them from the relevant WIS centre, i.e. Global Information System Centres (GISC) or Data Collection and Production Centres (DCPC).

4.5.2. Recording in Vol.C1

In addition, the Abbreviated Headings of Meteorological Bulletins are recorded in the Catalogue of Meteorological Bulletins (WMO Publication No. 9, Vol.C1). This enables any WMO Member to be aware of the availability of these bulletins and, if interested, to request them from the relevant Regional Telecommunication Hub (RTH). However, when DBNet products are embedded in “files” they are not systematically recorded in Vol. C1. In order to make the DBNet products more easily discoverable, it is recommended to record the DBNet bulletins in Vol.C1 even if embedded in a file.

The procedure for recording Meteorological Bulletins is described in: http://www.wmo.int/pages/prog/www/ois/Operational_Information/VolC1_en.html under “UPDATING PROCEDURES AND METHODS OF NOTIFYING THE WMO SECRETARIAT OF AMENDMENTS / ADVANCED NOTIFICATIONS”. The WMCs and RTHs on the Main Telecommunication Network (MTN) shall maintain Vol. C1 as regards bulletins issued from the zone for which they are responsible. The format to record a bulletin is described in: http://www.wmo.int/pages/prog/www/ois/Operational_Information/VolumeC1/AN_RecordFormat_en.html.

Table 9 provides guidance to complete the fields 9-15 of this record.

Field N°	Field	Value
9	Category	“E” (Essential data/products)
10	TTAAii	(Indicate TTAAii as defined by the DBNet coding
11	CCCC	(Indicate CCCC as defined by the DBNet coding convention)
12	CodeForm	“FM 94-XIV”
13	TimeGroup	"AS AVAILABLE"
14	Content	“DBNet”
15	Remarks	“TRANSMITTED AS A FILE”

Table 9: Guidance to record in Vol.C1 a DBNet bulletin sent as a file

4.6. PRODUCT DISTRIBUTION

The DBNet regional networks shall strive to make DBNet products available to the global user community and in particular to the NWP centres worldwide, through the WMO Information System.

The recommended route for DBNet data access within a region is to be defined at the regional level in consultation between the GISC/DCPC and the DBNet regional nodes taking into account the level of connectivity of the main regional users.

Inter-regional data exchange shall be implemented between regional nodes and GISCs, taking into account the recommendations of the GODEX-NWP group, which keep under review the requirements of NWP centres for inter-regional exchange of satellite data.

It will be the matter of a trade-off between the benefit provided by additional data and the resulting load on the telecommunications. While the primary distribution means will be the GTS/RMDCN networks), the use of a satellite broadcast service such as EUMETCast or CMACast or Internet is an advantage for users with limited WIS/GTS connectivity. A schematic illustration of the telecommunication scheme is provided in Figure 2.

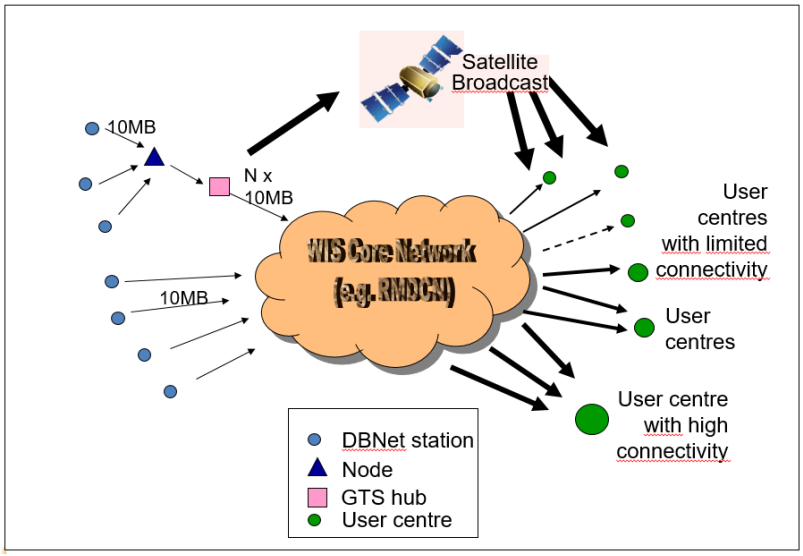


Figure 1: DBNet connectivity to GTS/RMDCN

Specific aspects of DBNet-WIS connectivity:

- DBNet stations with direct access to a core WIS node (GISC or DCPC) should directly inject into the WIS (e.g. Kyose/Tokyo, Crib Point/Melbourne);
- DBNet station with GTS access should directly inject into the GTS (e.g. New Delhi);
- DBNet station with no WIS/GTS access should send their products either to a GTS or WIS core node via FTP (e.g. Maupuia to Melbourne, Cordoba to Buenos Aires, Cachoeira Paulista to Brasilia, Jincheon to Seoul);
- As an alternative, DBNet stations which are part of a coordinated regional/sub-regional network should send their products to the regional/sub-regional node that will send the whole DBNet product package to a GTS hub/GISC/DCPC (e.g. EARS stations concentrated by EUMETSAT via VPN, before being sent to GISC/RTH Offenbach; Natal, Cuiaba via Cachoeira Paulista, before being sent to GISC/RTH Brasilia).

5. STANDARDS FOR SPECIFIC DBNet SERVICES

These standards and best practices are applicable to the provision of individual DBNet services. The DBNet services are defined in terms of groups of equivalent or similar instruments, potentially flying on different satellites. A particular DBNet operator may only provide a subset of the defined services. The scope of the overall DBNet includes the services listed in Table 2.

The areas covered by these standards are service-specific aspects of product processing, formats, quality control and monitoring.

5.1. IR/MW SOUNDING SERVICE

This service is provided for the ATOVS suite of instruments flying on NOAA/POES and EUMETSAT/Metop satellites as well as from equivalent instruments flying on CMA/FY-3 and NOAA/SNPP and JPSS satellites.

5.1.1. Product Processing Software

To ensure global consistency of the DBNet dataset, the DBNet operator shall make use of the AAPP (ATOVS and AVHRR Pre-processing Package) software for product processing for the ATOVS suite of instruments, of CSPP for ATMS and of the FY-3 L0/L1 pre-processing software package for MWTS, MWHS and IRAS.

The AAPP package is supplied and maintained by EUMETSAT's Numerical Weather Prediction Satellite Application Facility (NWP SAF). The package is freely available (subject to the signing of a license agreement) and the process for obtaining the package is fully described on the NWP SAF AAPP web pages (http://www.nwpsaf.eu). General background information on the AAPP software is also available on this web-page. The version of the AAPP software to be used shall be the latest release as defined on the AAPP web-page.

For changes affecting the data output, this latest release shall be implemented operationally within 1 month of release by the NWP SAF, otherwise the latest release shall be implemented operationally within 3 months.

For SNPP ATMS, The product processing shall be performed by AAPP and CSPP software. CSPP performs Level 1 processing which delivers Sensor Data Records (SDR) in HDF5 format for

ATMS. AAPP ingests these SDRs, and carries out BUFR encoding. CSPP can be downloaded from: http://cimss.ssec.wisc.edu/cspp/

FY-3 pre-processing software: FY-3 data are pre-processed by the FY3L0/L1pp software packages distributed by CMA, see http://satellite.cma.gov.cn/portalsite/ “Tools”.

AAPP can ingest the SDRs of MWTS, MWHS and IRAS, and can BUFR encode them.

5.1.2. Processing Level

Any products exchanged inter-regionally shall be at the level of brightness temperatures with geolocation on the original instrument grid.

5.1.3. Quality Checking and Quality Flags

The pre-processing software includes quality checking, and any products distributed shall include quality flags. For AMSU-A, MHS, HIRS and ATMS quality flags are available in the BUFR product. It must however be noted that currently (August 2016) quality flags are not available in the BUFR products for VASS (MWTS-2, MWHS-2 and IRAS), instead suspect measurements values are set to “missing”.

5.1.4. Product Quality Monitoring

Routine monitoring of DBNet IR/MW sounding data quality is performed by the NWP SAF. Monitoring results are available on the “Monitoring reports” section of the NWP SAF website http://www.nwpsaf.eu.

5.2. IR/VIS IMAGING SERVICE

5.2.1. Product Processing Software

For SNPP VIIRS, the product processing shall be performed by the CSPP software, followed by CVIIRS. For MERSI, the product processing shall be performed by the FY3L0/L1pp software packages.

For NOAA AVHRR, raw data are currently disseminated, therefore no product processing or encoding is required at this point in time (August 2016).

For Metop AVHRR, Metopizer or similar software is needed to first create EPS level 0.

5.2.2. Processing Level

The processing level shall be either raw HRPT (NOAA POES / Metop) or at the level of radiances/reflectivities (VIIRS / MERSI).

It is preferable for the orbit pass to be segmented to enable on-the-fly transmission of product segments in order to ensure low latency and to facilitate handling of large data sets.

As it is important to provide seamless imagery (without missing lines or overlaps) the acquisition schedules of the local stations shall be coordinated and where feasible the acquisition source shall be switched from one station to the next one at a defined imagery line.

Data compression is critical, efficient compression procedures shall be used. For VIIRS a compact SDR format has been developed and implemented in DBNet-EUMETSAT. This format provides a compact representation of VIIIRS Geolocation, Angular Information and Measurement Data. For further info see:
http://www.eumetsat.int/website/wcm/idc/idcplg?IdcService=GET_FILE&dDocName=PDF_VIIRS_SDR_PF_UG&RevisionSelectionMethod=LatestReleased&Rendition=Web.

5.2.3. Quality Checking and Quality Flags

Not applicable to raw data.

5.2.4. Product Quality Monitoring

Not applicable to raw data.

5.3. HYPERSPECTRAL IR SOUNDING SERVICE

5.3.1. Product Processing Software

For IASI EUMETSAT has implemented a computer at each station running AAPP together with the IASI Level 1 processor (OPS-LRS). Both AAPP and OPS-LRS are distributed by the NWP SAF (http://www.nwpsaf.eu/) and are freely available to any interested user. AAPP requires Metop Level 0 as input (Note: If not already delivered by the receiving station, the Level 0 can be generated by the "Metopizer" freeware available from EUMETSAT: http://www.eumetsat.int/website/home/Data/DataDelivery/SupportSoftwareandTools/index.html.

For OPS-LRS the IASI instrument auxiliary files are made available by the NWP SAF (www.nwpsaf.eu) to registered users of the package and announced via the NWP SAF AAPP Announcements Forum. Due to the interdependency between on-board instrument configuration and the on-ground processing software, it is essential that DBNet Station Operators install the updated auxiliary files into AAPP before corresponding on-board configuration changes are uploaded to Metop by EUMETSAT operations. Details on the installation process are found in the OPS-LRS User Manual.

For SNPP CrIS, the product processing shall be performed by AAPP and CSPP software. CSPP performs Level 1 processing which delivers Sensor Data Records (SDR) in HDF5 format for ATMS, CrIS and VIIRS instruments. AAPP ingests these SDRs, performs CrIS channel selection, and BUFR encodes. CSPP can be downloaded from: http://cimss.ssec.wisc.edu/cspp/

For HIRAS the availability of a product processing package has not yet been confirmed.

5.3.2. Processing Level

Any products exchanged inter-regionally shall be at channel subset of level 1 radiances, optionally supplemented with Principal Component (PC) Scores that allow a reconstruction of the full spectra

with minimal loss of information. The definition of the set of selected channels for each of the hyperspectral sounders as well as the selection of the appropriate PC score representation is performed by the agencies, in consultation with users, according to the following table.

Service	Channel selection responsible	PC score selection responsible	Apodization applied
IASI	EUMETSAT	EUMETSAT	Yes
CrIS	NOAA	TBD	Yes
HIRAS	CMA	TBD	Yes
AIRS	NOAA	N.A.	No

Table 10: Data selection for hyperspectral sounders

In brief, at the PC encoding step each spectrum is projected onto a set of orthogonal basis functions (eigenvectors) and the resulting amplitudes are the PC scores. In a reverse process, the DBNet user can reconstruct radiances when he has the PC scores and the eigenvectors. The number of PCs is defined by the agency, with the aim to preserve as much as possible of the real atmospheric signal, while discarding PCs that contain only instrument noise.

For information on the implementation of PC scores in AAPP, please see the document NWPSAF-MO-UD-022 “IASI Principal Components in AAPP: User Manual”, available from http://www.nwpsaf.eu/deliverables/aapp/index.html.

Regarding channel selection for CrIS, NOAA has documented a recommended channel selection of 399 channels, in "Methodology and Information Content of the NOAA NESDIS Operational Channel Selection for the Cross-Track Infrared Sounder (CrIS)” by Antonia Gambacorta and Christopher D. Barnet. IEEE Transactions on Geoscience and Remote Sensing, Vol. 51, No. 6, June 2013.

Regarding channel selection for IASI, EUMETSAT has documented a recommended channel selection of 500 channels in the IASI Level 1 Product Guide http://www.eumetsat.int/website/wcm/idc/idcplg?IdcService=GET_FILE&dDocName=pdf_iasi_level_1_prod_guide&RevisionSelectionMethod=LatestReleased&Rendition=Web.

The channel selections for the hyper-spectral IR sounders will be revisited in the future based on increasing capabilities of the users, improved WIS capacity for global product distribution and changes in instrument capability (for example upon transition from SNPP to NOAA-20).

5.3.3. Quality Checking and Quality Flags

The processing software includes quality checking, and any products distributed shall include quality flags. For IASI and CrIS all quality flags in the native sounder products formats are transferred to the BUFR formatted product.

5.3.4. Product Quality Monitoring

Routine monitoring of DBNet hyperspectral sounding data quality is performed by the NWP SAF. Monitoring results are available on the "Monitoring reports" section of the NWP SAF web site http://www.nwpsaf.eu. Consistency between global and local data products is monitored, and also the consistency between raw and reconstructed radiances.

5.4. SCATTEROMETRY SERVICE

This service is currently provided by the EUMETSAT EARS network for the ASCAT instrument flying on Metop-A/B.

5.4.1. Product Processing Software

For ASCAT, the processing software used is the ASCAT Level 1 Product Processing Facility (PPF) software, ported from the EUMETSAT EPS Central Ground Segment.

Availability of a Wind RAD (FY-3) processing package has not yet been confirmed

5.4.2. Processing Level

Any products exchanged inter-regionally shall be at level 1 (backscatter cross-sections) or at level 2 (winds and soil moisture).

5.4.3. Quality Checking and Quality Flags

The pre-processing software includes quality checking, and any products distributed shall include quality flags.

5.4.4. Product Quality Monitoring

TBD

5.5. MW IMAGERY SERVICE

This service is currently not provided, but is under consideration for the MWRI instrument on FY-3.

5.5.1. Product Processing Software

Availability of a MWRI processing package has not yet been confirmed

5.5.2. Processing Level

TBD

5.5.3. Quality Checking and Quality Flags

The pre-processing software includes quality checking, and any products distributed shall include quality flags.

5.5.4. Product Quality Monitoring

TBD

6. CONCLUSION

The provisions contained in this document contain the standards to be followed by DBNet Operators to:

- Ensure that an appropriate level of service is provided regionally;
- Facilitate the inter-regional exchange of DBNet data;
- Ensure the global consistency of the DBNet datasets.

ANNEXES

A. TERMS OF REFERENCE OF THE DBNet COORDINATION GROUP

1. A DBNet Coordination Group is established by the WMO Space Programme in order to support the development and implementation of the Direct Broadcast Network for Acquisition and Near Real-Time Relay of Low Earth Orbit Satellite data (DBNet).

2. The aim of the DBNet Coordination Group is:

    - To keep under review the High-Level Specifications of DBNet Services, in consultation with the users;
    - To coordinate the implementation and expansion of DBNet Services responding to the user needs;
    - To define and maintain the standards ensuring interoperability and Inter-regional exchange of DBNet products, and the consistency with the WMO Information System;
    - To monitor the performance of DBNet components and define actions to improve this performance as appropriate;
    - To keep under review the priorities for filling coverage gaps and for scheduling the acquisition of satellite data;
    - Identifying issues to be submitted for consideration by CGMS satellite operators.

3. The DBNet Coordination Group is composed of DBNet regional or subregional network coordinators, organizations providing software for L0/L1 processing, technical experts designated by organizations contributing to the global DBNet network, planning or considering to contribute to it, and the WMO Secretariat.

4. A focal point is designated within the DBNet CG to ensure liaison with IPET-DRMM.

5. The DBNet Coordination group meets nominally once a year, or more frequently if necessary.

6. The DBNet Coordination Group reports on its activities to CGMS and to the WMO Commission for Basic Systems through the Inter-Programme Expert Team on Satellite Utilization and Products (IPET-SUP). It receives guidance from CGMS, from CBS through IPET-SUP, and from representative user groups such as the International TOVS Working Group (ITWG).

B. PROCEDURE FOR ADDING/MODIFYING A STATION IN THE DBNet NETWORK

The purpose of this procedure is to guide the station operator on the steps to be followed when including a new station in the DBNet network, or modifying the operation mode of a station, ensuring appropriate coordination and information of all parties involved.

The following steps shall be followed for adding a new station:

Step 1: The Station Operator (or the regional/subregional coordinator) informs the WMO Space Programme Office (WMOSP) of the WMO Secretariat of the characteristics of the new DBNet station:

- Latitude and Longitude of the station (in degrees, with decimals);
- Name of the station;
- Three-letter abbreviated name;
- Centre administratively responsible for this station;
- Identifier of the centre in Common Code Table (CCT) C-1/C-11 (if available);
- Identifier of the station as sub-centre of this centre in CCT C-12 (if available);
- RTH/GISC which will transmit the data over the GTS/WIS Core Network;
- CCCC identifier of this RTH/GISC;
- DBNet Services which will be supported by the station.

Step 2: If the Centre is not yet identified in CCT C-11, or if the station is not yet identified in CCT C-12 as a sub-centre of this centre, the operator requests the addition of a code for the centre and/or the sub-centre in the relevant Common Code Tables. The procedure for amending the tables is to send a request from the Permanent Representative (PR) to the Secretary-General, or from the focal point for codes and data representation matters of the country/territory to the WMO Secretariat (OBS/WIS/DRMM with copy to OBS/SAT). The procedures for amending the tables are initiated after each update implementation in May and November.

Step 3: The Operator implements the operational processes for acquisition, pre-processing, processing, coding and routing of DBNet products in accordance with the applicable DBNet standards defined in Sections 3 and 4.

Step 4: The Station operator sends file samples by FTP for validation during a minimum test period of one week:

- To the RTH in charge of transmitting the data into the GTS (if different from the Operator);
- To the relevant DBNet regional coordinating center;
- To the DBNet monitoring centre.

Step 5: The RTH, the Regional Coordinator check the consistency with DBNet conventions and regularity and timeliness of the products. The Global DBNet Monitoring centre checks the consistency of the products with global data and their timeliness. They interact as appropriate with the Station Operator until full compliance is demonstrated.

Step 6: Once the test is successful, the Operator:

- Informs the WMO Space Programme Office of the planned start of the routine dissemination, and of any change to the bulletin headings and file naming (if relevant);
- Requests the responsible RTH Focal Point in an appropriate manner so that the Focal Point can update relevant parts of the Vol. C1 with respect to the new bulletins at least two months in advance. A/N (advanced notification) of Vol. C1 will be released to WMO Members;
- Updates the discovery metadata record to share with the responsible DCPCs or GISCs.

Step 7: The PR of the Operator's country/territory or the regional/subregional coordinator informs the WMO Secretariat of changes to the DBNet operation and provides input for inclusion of an announcement in the World Weather Watch Operational Newsletter (http://www.wmo.int/pages/prog/www/ois/Operational_Information/index_en.html); the Secretariat, updates the DBNet documentation accordingly and takes any other appropriate action to inform the satellite community.

In case of modification or termination of a DBNet station operation, the Operator informs the Space Programme Office of any change of status of the station, for instance if an additional DBNet Service is ready to be implemented at the station. The production associated with the new Service is implemented following Steps 3 to 7 above.

If a Service is cancelled, or the overall operation of a station is terminated, the Operator:

- Informs the WMO Space Programme Office of the planned termination;
- Records the end of the bulletins in Vol. C1;
- Deletes the discovery metadata record.

The WMO Space Programme Office updates the DBNet documentation accordingly.

C. DBNet RECEPTION SCHEDULING PRIORITIES

Last update: May 2015

Satellite	**Orbit and satellite status** (D=descending, A=ascending)	**Instrument health**	**Global data** (DBNet impact is largest when global data are late)	**Direct broadcast transmission**	**DBNet priority** (H/M/L)
SNPP	NOAA Prime Polar Orbiter PM 1330A	Good	1 dump per orbit	Good (X-band). Occasional short gaps due to solar array obscuration.	H
Metop-B	Primary AM service. 0930D	Good	Very good: Arctic and Antarctic dumps	Good (L-band)	H
NOAA-19	Prime NOAA Services Mission PM. Close to SNPP 1400A/0200D	Good	1 dump per orbit	Good (L-band)	H
NOAA-18	Has drifted to an early morning orbit 1700A/0500D	Good. HIRS degraded	Some blind orbits	Good (L-band)	H
Metop-A	Same orbital plane as Metop-B 0930D	Good	1 dump per orbit	Limited geographically	M
NOAA-15	Close to NOAA-18 0530D	Poor. AMSU-B and HIRS not working. AMSU-A is still useful.	Some blind orbits. Low priority in NESDIS L1 processing.	Poor signal strength (L-band), can only be received by large dishes	L
FY-3C	1030D	MWTS-2 not working, MWHS-2 OK.	Significant delays	Good (L-band for sounders, X-band for MERSI)	L

D. EXTRACT OF THE MANUAL ON CODES: EXTRACT OF COMMON CODE TABLE C-13

The present extract contains the satellite-related entries as of August 2015.

Link to Current version:
http://www.wmo.int/pages/prog/www/WMOCodes/WMO306_vI2/LatestVERSION/WMO306_vI2_CommonTable_en.docx

Data categories		**International data sub-categories**	
BUFR Edition 4 Octet 11 in Section 1		BUFR Edition 4 Octet 12 in Section 1	
Code figure	**Name**	**Code figure**	**Name (corresponding traditional alphanumeric codes are in brackets)**
3	Vertical soundings (satellite)	0	Temperature (SATEM)
		1	TIROS (TOVS)
		2	ATOVS
		3	AMSU-A
		4	AMSU-B
		5	HIRS
		6	MHS
		7	IASI
		20	IR temperature/humidity sounding
		30	Hyperspectral temperature/humidity sounding
		40	MW temperature/humidity sounding
		50	Radio occultation sounding
12	Surface data (satellite)	0	ERS-uwa
		1	ERS uwi
		2	ERS-ura
		3	ERS-uat
		4	SSM/I radiometer
		5	Surface temp./radiation (SATOB)
		6	Quikscat
		7	ASCAT data
		8	Soil moisture
		9	Normalized differential vegetation index (NDVI)
		10	Normalized radar backscatter
		11	Surface emissivity
		12	Sea surface temperature

21	Radiances (satellite measured)	0	Earth radiation budget
		5	Cross-track infrared sounder (CrIS)
		6	Advanced technology microwave sounder (ATMS)
		7	Visible/infrared imager radiometer suite (VIIRS)
22	Radar (satellite) but not altimeter and scatterometer	0	Cloud and precipitation radar
		1	Synthetic aperture radar
23	Lidar	0	Lidar based missions (for wind, for cloud/aerosol, for water vapour, for altimetry)
24	Scatterometry (satellite)	0	Wind scatterometry
25	Altimetry (satellite)	0	Radar altimetry
26	Spectrometry (satellite)	0	Cross nadir shortwave spectrometry (for chemistry)
		1	Cross nadir IR spectrometry (for chemistry)
		2	Limb sounding shortwave spectrometry
		3	Limb sounding IR spectrometry
		4	Limb sounding sub-millimetre wave spectrometry
30	Calibration dataset	0	Sub-setted data
		1	Collocated data
		2	On-board calibration data
		3	Bias monitoring
		4	Near real-time correction
		5	Re-analysis correction
101	Image data (satellite)	0	Multi-purpose VIS/IR imagery
		1	Conical scanning MW imagery (intermediate frequencies)
		2	Low frequency MW imagery
		3	Ocean colour imagery
		4	Imagery with special viewing geometry
		5	Lightning imagery
		6	High-resolution shortwave imagery for land observation
		7	SMOS data

E. EXISTING/PROPOSED CODE VALUES FOR INSTRUMENTS USED IN DBNet

"A_1" Data type designator in GTS Headings "T_1 T_2 A_1 A_2ii" defined in the Manual on the GTS, WMO-No. 386 Vol. 1 [AD.2] See current values in Table C6 in the Explanation of Data Designators: http://www.wmo.int/pages/prog/www/ois/Operational_Information/Publications/WMO_386/AHLsymbols/TableDefinitions.html		
Definition	Comment	Corresponding category/sub-category in CCT C-13 (WMO-No. 306) [AD.1]
With T_1 T_2 =IN : **A AMSU-A** **B AMSU-B** **C CrIS (selected channels)** **H HIRS** **I IRAS** **J HIRAS** **K MWHS/MWHS-2** **M MHS** **Q IASI (PC scores)** **S ATMS** **T MWTS/MWTS-2**	Level 1 sounding products (Code values extracted from Table C6 as of 1/01/2016)	 003 / 03 003 / 04 021 / 05 003 / 05 003 / 20 003 / 30 003 / 40 003 /0 6 003 / 07 021 / 06 003 / 40
Additional codes (for information only)		
With T_1 T_2 =IE: A AMSU-A/METOP D IASI L2 products H HIRS/METOP M MHS/METOP Q IASI (PC scores)	Used by EUMETSAT with T_1T_2 =IE for products from EUMETSAT satellites.	 003 / 03 003 / 07 003 / 05 003 / 06 003 / 07

_____

F. PRODUCT IDENTIFIER FOR DBNet PRODUCT FILENAMES

Product identifier = <location indicator>, <data designator>, <free description> **In the filename structure defined in the Manual on the GTS [AD.2]**		
DBNet convention for the location indicator	**DBNet convention for the data designator**	**DBNet convention for the free description**
<Country ID - Organization- Production Centre>	<instrument> Where: IASI = iasi CrIS = cris ATMS = atms MWTS = mwts MWHS = mwhs IRAS = iras HIRAS = hiras AMSU-A = amsua AMSU-B = amsub MHS = mhs	"DBNet+<satellite>+<station>" Where <satellite> is: NOAA-xx = noaaxx METOP-A = metopa METOP-B = metopb Suomi-NPP = snpp FY-3A = fy3a FY-3B = fy3b FY-3C = fy3c FY-3D = fy3d JPSS-1 = noaa20 JPSS-2 = noaa21 Where <station> is the Direct Broadcast receiving station (same as "Originating sub-centre" in the BUFR Section 1)
For example: "br-inpe-cpt" for a product generated by INPE in Cachoeira Paulista (Brazil)		Example: "DBNet+metopb+ath" for a DBNet product generated with METOP-B data received in Athens.

[Note: More explanations on "Accumulating messages into files can be found in the Manual on the GTS (WMO-No. 386) Vol.1, Part II, Attachment II-15, as of page 158]

[Note: the identifiers "rars" and "npp" are accepted as alternatives to "DBNet" and "snpp" for backward compatibility]

G. GLOSSARY

ATOVS	Advanced TIROS Operational Vertical Sounder (instrument package including HIRS, AMSU-A and AMSU-B)
CCSDS	Consultative Committee for Space Data Systems (http://public.ccsds.org/default.aspx); “CCSDS” also designates the data format standard defined by this committee.
CCSDS to L0	The conversion from CCSDS to EPS level 0 is generally included in the receiving station software. It is also available from EUMETSAT as part of the « Metopizer » software.
CDA	Command and Data Acquisition station, major ground facility of a Low Earth Orbit satellite programme
CSPP	Community Satellite Processing Package provided by NOAA through the University of Wisconsin for Direct Broadcast users.
DBNet Coordinator	Regional coordinator in charge of providing technical guidance to operators, monitoring the timeliness, and maintaining on line information for users, for a regional component of the global DBNet network
DBNet Monitoring centre	Organization in charge of DBNet product quality monitoring at the global scale (NWP SAF, Met Office/UK)
DBNet Operator	Organization responsible for data acquisition and pre-processing
DBNet Station	Facility including a Direct Readout station that acquires the data
DBNet:	Direct Readout Acquisition and Relay System for LEO Satellite Data. It is a system based on the concept of RARS, but expanded to address a broader range of data and products, and a variety of formats and protocols while complying with a set of standards and best practices which are described in the present guide.
EPS	EUMETSAT Polar System
GISC	Global Information System Centre
GODEX-NWP	Group for establishing and maintaining requirements for Global Data Exchange for NWP centers
HIRLAM	High Resolution Limited Area Model, developed and maintained through a cooperation of European meteorological institutes for operational short-range weather forecasting.
ITWG	International TOVS Working Group
JPSS	Joint Polar System Satellite programme. The JPSS-1 and JPSS-2 satellites of the JPSS programme will be renamed NOAA-20 and NOAA-21 after successful launch.

LEO	Low Earth Orbit
NWP	Numerical Weather Prediction
OPS-LRS	IASI “Operation Software for Local Reception Station”, which processes IASI instrument data from Level 0 (raw instrument data) through to level 1c (calibrated, geolocated, Gaussian-apodised radiances). OPS-LRS is provided by EUMETSAT through the NWP SAF as part of the AAPP deliverable.
PFS	Product Format Specification (EUMETSAT)
RARS	Regional ATOVS Retransmission Service. It is an arrangement among HRPT station operators to acquire, pre-process, and share satellite sounding data from ATOVS instrument package aboard NOAA and METOP satellites, in near real-time, in accordance with agreed standards, in support of NWP.
RDR	Raw Data Record
RMDCN	Regional Meteorological Data Communication Network
RTH	Regional Telecommunication Hub of the Global Telecommunication System (GTS)
RT-STPS	Real-time Software Telemetry Processing System, a generalized CCSDS data processing package that ingests telemetry data from a spacecraft transmission in real-time, performs multi-mission protocol processing, and produces output to a file or TCP/IP socket. RT-STPS is provided by the NASA Direct Readout Laboratory.
SDR	Sensor Data Record
SNPP	Suomi National Polar-orbiting Partnership
WIS	WMO Information System
WMOSP	WMO Space Programme Office, within the WMO Observing and Information Systems Department (OBS/SAT)

_____

Annex 5

AMEND THE *MANUAL ON THE GTS* (WMO-No. 386), ATTACHMENT I-5 AS FOLLOWS

[The following text is copied from Annex 1 to Recommendation 3.5/1 (CBS-16). Amendments in this Annex apply to WMO-No. 386 Manual on the Global Telecommunication System]

1 In Attachment I-5 Section 4 (Priorities)

Add a note after the list of information types in paragraph 4.1:

Note: Reference to report types includes any World Weather Watch code form representation of that information.

Amend paragraph 4.2 to read:

4.2 Monitoring of satellite data presents a special case. There are only a few operators and their standards for monitoring, including quality control of satellite data, are already high. Monitoring of satellite data bulletins and ~~GRID~~ GRIB code bulletins shall be a special event for a limited time as designated by the WMO Secretariat.

2 In Attachment I-5 Section 5 (Responsibilities)

Amend paragraph 5.5 to read:

5.5 In order to keep under review the efficient operation of the WWW, internationally coordinated monitoring on a non-real-time basis should be carried out periodically ~~once~~ four times a year in October, January, April and July, on the full range of global on the full range of global observational data and with the participation of a limited number of major WWW centres. During other periods, particular problem areas should be monitored, in respect of either selected information only or limited parts of the world. The Secretary-General will arrange, in consultation with the appropriate centres, details of the special monitoring exercises and the periods during which they should be carried out, and will provide adequate notice well in advance.

3 In Attachment I-5 Section 6 (Procedures)

Amend paragraph 6.1 and 6.2 to read:

6.1 As far as real-time monitoring is concerned, each centre should develop the necessary detailed procedures for this purpose. These procedures will vary from centre to centre, but should be designed to facilitate the real-time checking of the receipt of bulletins and observations as appropriate. At fully automated centres, these procedures may include the use of telecommunication system records~~, visual display units, special programmes in telecommunication and data-processing computers, and so on~~. At manual centres, check lists or sheets may be developed for the same purposes using ticks, crosses or the entry of times to indicate when selected bulletins and/or reports have been received. ~~To avoid excessive use of paper forms, it may be convenient to place transparent sheets of plastic over the check sheets and make entries using soft wax pencils.~~ The entries can be removed very easily when a suitable period has elapsed and the sheets made ready for the checks to be repeated for a later period. Some further guidance on the operation of real-time monitoring, together with examples of the kind of forms which might be developed, are given in Table C.

6.2 As far as non-real-time monitoring is concerned, when special exercises are requested by the Secretariat, an indication of the form in which contributions should be made will be provided at the time the request is made. It is important that, as far as possible,

centres should follow closely the procedures indicated in order that results from various centres be directly comparable with each other. It is particularly important that this should be the case when the annual global monitoring exercise is carried out. The procedures, together with the standard ~~forms~~ formats to be used for the provision of results, are given in Table D.

4 In Attachment I-5 Table C (Guidance for real-time monitoring)

Add a note immediately following the title of Table C:

Note: In this Table, reference to a report type (such as SYNOP) refers to that information in any WWW code form.

5 In Attachment I-5 Table D (Procedures for internationally coordinated non-real-time monitoring)

Amend paragraph 1 Monitoring Periods to read:

The internationally coordinated monitoring of data for global exchange will be carried out ~~once~~ four times a year in October, January, April and July with a view to check periodically the efficiency of the operation of the WWW. Statistics should be compiled ~~by manually operated and automated centres~~ for the periods ~~1–5 October and~~ 1–15 October, 1-15 January, 1-15 April and 1-15 July. ~~In order to facilitate the comparison of results between manually operated and automated centres, automated centres should also provide results for the two periods of 1–5 October and 1–15 October.~~

~~Note: As regards CLIMAT, the monitoring period should be extended to 15 days, even if (for other observations) a return for a period of only five days is made.~~

Amend paragraph 2 (Types of data to be monitored) to read:

The types of data listed in the following table should be monitored:

Types of data	*Abbreviated headings of bulletins* $T_1T_2A_1A_2$	*Reference format for presentation of results (See http://wis.wmo.int/iwm)*
SYNOP reports	$SMA_1A_2/ISMA_2/ISNA_2$	A
Parts A and B of TEMP reports	$USA_1A_2/UKA_1A_2/IUKA_2$	B1/B2
Parts A and B of PILOT reports	$UPA_1A_2/UGA_1A_2/IUJA_2$	B1/B2
SHIP reports	$SMA_1A_2/ISSA_2$	C1/C2
Parts A and B of TEMP SHIP reports	$USA_1A_2/UKA_1A_2/IUKA_2$	D1/D2/D3/D4
Parts A and B of PILOT SHIP reports	$UPA_1A_2/UGA_1A_2/IUJA_2$	D5/D6/D7/D8
BUOY reports	$SSA_1A_2/IOBA_2$	E
AIREP reports	$UAA_1A_2/IUAA_2$	F
AMDAR reports	$UDA_1A_2/IUAA_2/IUOA_2$	G
BATHY/TESAC/TRACKOB reports	$SOA_1A_2/IOSA_2$	H
CLIMAT reports	$CSA_1A_2/ISCA_2$	I1

(a) Monitoring of SYNOP reports

For each monitored station identified by the WIGOS station identifier and, if it exists, the World Weather Watch station index number (IIiii), the number of SYNOP reports made at ~~the main standard synoptic hour hours (0000, 0600, 1200 and 1800 UTC)~~ and available during the monitoring period within one hour, 2 hours and 6 hours of the standard bulletins times should be ~~inserted in the appropriate columns of Format A~~ recorded in the relevant file defined in http://wis.wmo.int/iwm;

(b) Monitoring of Parts A and B of TEMP and PILOT reports (or ascent to 100mb for reports in Table Driven Code Forms)

For each monitored station identified by the WIGOS station identifier and, if it exists, the World Weather Watch station index number (IIiii), the number of parts A and B of TEMP and PILOT reports (made by tracking a free balloon by electronic or optical means ~~at the main standard synoptic hours (0000, 0600, 1200 and 1800 UTC~~) and available during the monitoring period within 2 hours and 12 hours of the standard bulletin times should be inserted in the ~~appropriate columns of the forms, formats B1 and B2~~ recorded in the relevant file defined in http://wis.wmo.int/iwm;

(c) Monitoring of SHIP reports

The number of bulletins identified by their abbreviated headings (T1T2A1A2ii CCCC) including SHIP reports ~~made at the main synoptic hours (0000, 0600, 1200 and 1800 UTC)~~ and available during the monitoring period within 2 hours and 12 hours of the standard bulletin times with the number of reports included in these bulletins should be recorded in the relevant file defined in http://wis.wmo.int/iwm;

(d) Monitoring of parts A and B of TEMP SHIP and PILOT SHIP reports (or ascent to 100mb for reports in Table Driven Code Forms)

The number of bulletins identified by their abbreviated headings (T1T2A1A2ii CCCC) including parts A and B of TEMP SHIP and PILOT SHIP reports (or ascent to 100mb for reports in Table Driven Code Forms) ~~made at the main synoptic hours (0000, 0600, 1200 and 1800 UTC)~~ and available during the monitoring period within 12 hours and 24 hours of the standard bulletin times with the number of reports included in these bulletins, should be ~~inserted in the appropriate columns of the forms, formats D1 to D8~~ recorded in the relevant file defined in http://wis.wmo.int/iwm;

(e) Monitoring of BUOY, AIREP and AMDAR reports

The number of bulletins identified by their abbreviated headings (T1T2A1A2ii CCCC) including BUOY, AIREP and AMDAR reports compiled between 2100 to 0259 UTC, 0300 to 0859 UTC, 0900 to 1459 UTC and 1500 to 2059 UTC and available during the monitoring period before 0500, 1100, 1700 and 2300 UTC, respectively, as well as the number of reports included in these bulletins, should be ~~inserted in the appropriate columns of the forms, formats E, F and G~~ recorded in the relevant file defined in http://wis.wmo.int/iwm;

(f) Monitoring of BATHY/TESAC/TRACKOB

The time of receipt of bulletins identified by their complete abbreviated headings (T1T2A1A2ii CCCC YYGGgg (BBB)) containing BATHY/TESAC/TRACKOB reports as well as the number of reports included in these bulletins should recorded in the relevant file defined in http://wis.wmo.int/iwm;

(g) Monitoring of CLIMAT reports

For each station monitored and identified by the WIGOS station identifier and, if it exists, the World Weather Watch station index number (IIiii), "I" should be recorded in the relevant file defined in http://wis.wmo.int/iwm.

Amend paragraph 5 (Implementation of monitoring procedures and questionnaires) to read:

5.1 A questionnaire ~~Questionnaires~~ related to the procedures implemented at the centres, ~~suspension of observing programmes at observing stations and suspension of~~

~~transmission on circuits are~~ is provided in the section "Questionnaire on the implementation of the monitoring procedures" at http://wis.wmo.int/iwm. ~~given in formats J, K and L, respectively.~~

5.2 Monitoring procedures should be implemented at centres in such a way that all replies to the questions included in the questionnaire ~~format J~~ should be positive (reply: 1 ~~Yes~~). ~~Questions 7, 8 and 10 are only applicable to SYNOP, TEMP, PILOT and CLIMAT reports.~~

Amend paragraph 6.1 (Standard format for the statistics) to read:

6.1 With a view to enabling the easy comparison of results of internationally coordinated monitoring carried out by the different centres, the standard formats ~~attached at~~ specified in http://wis.wmo.int/iwm should be used. All centres carrying out monitoring should state clearly the period covered. In each format, centres should present the results region by region as well as for the Antarctic and give totals of the number of bulletins or reports received within the specified time region by region and for the Antarctic.

Delete paragraph current paragraph 6.2 and re-number paragraph 6.3 to 6.2.

Delete the format tables A to L inclusive (pages 34 to 55 of the English edition)

_____

[The following text is copied from Annex 2 to draft Recommendation 3.5/1 (CBS-16)]

1. Amend Part 1, Section 1, paragraph 1.1 as follows

1.1 Functions

The functions of the Global Telecommunication System (GTS) as a key component within the WMO Information System (WIS) shall be to facilitate the flow of data and processed products to meet the WWW requirements in a timely, reliable and cost effective way, ensuring that all Members have access to data and products in accordance with approved procedures and within the limits of the agreed WWW system.

Note: It also gives telecommunication support to other programmes as a part of WIS and as decided by the WMO Congress or the Executive Council, within the limits of its primary objectives.

2. Amend Part 1, Section 1, paragraph 1.2.1 as follows

1.2.1 The Global Telecommunication System shall be so organized as to accommodate the volume of meteorological information and its transmission within the required time limits as the core network of WIS and to meet the needs of World, Regional Specialized and National Meteorological Centres, resulting from the implementation of the WWW.

Insert note after paragraph 1.2.2(c) to read

1.2.2 The GTS shall be organized on a three-level basis, namely:

… (c) The national telecommunication networks.

Note: The components of the MTN connecting the WIS Global Information System Centres is also referred to as the WIS Core Network (See the *Manual on the WMO Information System* WMO-No. 1060)

3. Amend Part 1, Section 3 as follows

3. FUNCTIONS AND CHARACTERISTICS OF THE NETWORKS OF THE GLOBAL TELECOMMUNICATION SYSTEM

3.1 The Main Telecommunication Network (MTN)

3.1.1 The MTN shall be an integrated system of circuits linking together the GISCs on the WIS Core Network ~~WMCs~~ and designated RTHs. ~~The circuits which directly link WMCs and/or RTHs situated on the MTN may, at the request of Members concerned, be designated as circuits of the MTN.~~

Note: The names of these centres, together with a diagram indicating the configuration of the MTN, are given in Attachment I-2.

3.1.2 The MTN shall be designed in such a way that the traffic originating from each centre (WMC, designated RTH) will be routed selectively towards the addressee centre(s). Each centre on the MTN shall ensure selective relay of the traffic which it receives towards the circuit(s) which it serves.

3.1.3 The MTN shall have the function of providing an efficient, reliable communication service between the designated centres, in order to ensure:

(a) Rapid and reliable exchange of observational data required to meet the GDPFS requirements;

(b) Exchange of processed information between the WMCs, including data received from meteorological satellites;

(c) Transmission of processed information produced by the WMCs, to meet the requirements of RSMCs and NMCs;

(d) Transmission of other observational data and processed information required for interregional exchange.

Note: Responsibilities of RTHs, including those ~~centres~~ located on the MTN, for the transmission of observational data and processed information are given in Attachment I-3.

4. Amend Part 1, Attachment I-2 by replacing the existing diagram with the following diagram (Figure 1 WIS RTH routeing) as follows

Attachment I-2. CONFIGURATION OF THE MAIN TELECOMMUNICATION NETWORK

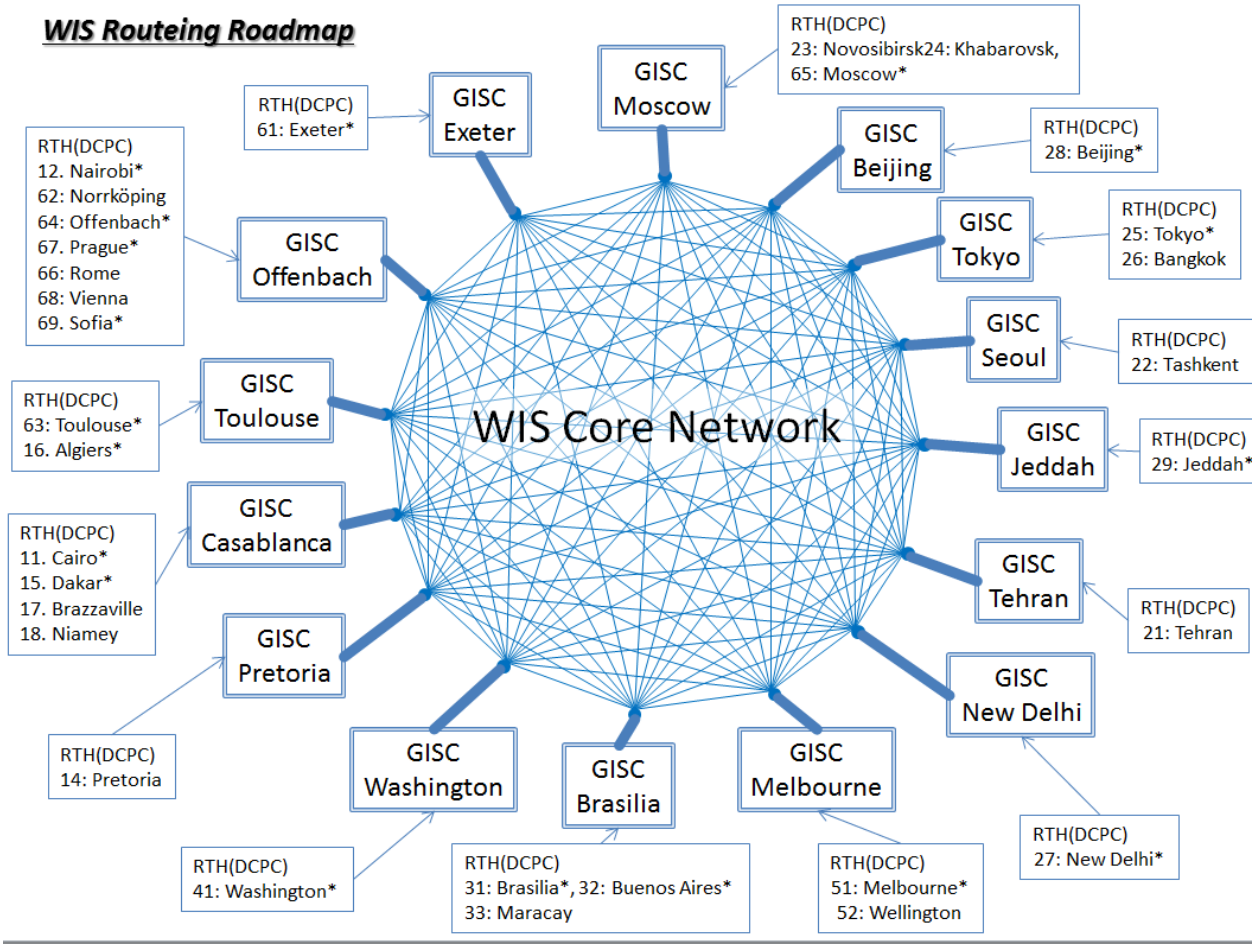


Figure 1 WIS RTH routeing plan

5. Amend Part 1, Attachment I-3 as follows

ATTACHMENT I-3. RESPONSIBILITIES OF REGIONAL TELECOMMUNICATION HUBS ~~CENTRES ON THE MAIN TELECOMMUNICATION NETWORK~~ FOR THE TRANSMISSION OF OBSERVATIONAL DATA AND PROCESSED INFORMATION

1. RESPONSIBILITIES FOR THE COLLECTION, EXCHANGE AND DISTRIBUTION OF OBSERVATIONAL DATA OF ~~WMCs AND~~ RTHs ~~LOCATED ON THE MAIN TELECOMMUNICATION NETWORK~~

~~The responsibilities are~~

[Replace the table under 1. with the following table shown in Figure 2 (RTH - Areas of Responsibility)]

RTH Region	RTH Reference No.	RTH City (Country) (*=RTH/MTN)	RTH's Principal GISC	RTH's Backup GISC	RTH's Area of Responsibility
1	11	Cairo* (Egypt)	Casablanca	Toulouse	Egypt, Sudan, Libya, adjacent sea areas
1	12	Nairobi* (Kenya)	Offenbach	Moscow / Tokyo	Kenya, Ethiopia, Burundi, Djibouti, Uganda, Rwanda, Somalia, La Réunion, United Republic of Tanzania, adjacent ocean areas
1	13	Lusaka (Zambia)	Pretoria	Exeter	Zambia, Zimbabwe, Malawi
1	14	Pretoria (South Africa)	Pretoria	Exeter	South Africa, Angola, Botswana, Lesotho, Madagascar, Malawi, Mozambique, Namibia, Swaziland, La Réunion, Zimbabwe, and the following centres via La Réunion: Antananarivo, Comoros, Mauritius, Seychelles, Amsterdam island, Kerguelen, adjacent ocean areas
1	15	Dakar* (Senegal)	Casablanca	Toulouse	Senegal, Ascension Island, Cabo Verde, Canary Islands, Cote d'Ivoire, Guinea, Guinea-Bissau, Liberia, Madeira, Mali, Mauritania, Morocco, Nigeria, Sierra Leone, St. Helena, The Gambia, adjacent ocean areas

RTH Region	RTH Reference No.	RTH City (Country) (*=RTH/MTN)	RTH's Principal GISC	RTH's Backup GISC	RTH's Area of Responsibility
1	16	Algiers* (Algeria)	Toulouse	Exeter	Algeria, Morocco, Lebanon, Tunisia, adjacent sea areas
1	17	Brazzaville (Congo)	Casablanca	Toulouse	Republic of the Congo, Cameroon, Central African Republic, Gabon, Equatorial Guinea, São Tomé and Príncipe, Democratic Republic of the Congo, adjacent ocean areas
1	18	Niamey (Niger)	Casablanca	Toulouse	Benin, Burkina Faso, Chad, Ghana, Niger, Nigeria, Togo
2	21	Tehran (Islamic Republic of Iran)	Tehran	TBD	Iran (Islamic Republic of), Iraq, Pakistan, Yemen, other Arabian territories, adjacent sea and ocean areas
2	22	Tashkent (Uzbekistan)	Seoul	Moscow	Afghanistan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan
2	23	Novosibirsk (Russian Federation)	Moscow	Offenbach / Toulouse	Mongolia, Russian Federation (in Region II)
2	24	Khabarovsk (Russian Federation)	Moscow	Offenbach / Toulouse	Democratic People's Republic of Korea, Russian Federation (in Region II), adjacent sea and ocean areas
2	25	Tokyo* (Japan)	Tokyo	Beijing / Offenbach / Melbourne	Hong Kong(China), Japan, Macao(China), Republic of Korea, adjacent sea and the Pacific Ocean areas
2	26	Bangkok (Thailand)	Tokyo	Beijing / Offenbach / Melbourne	Cambodia, Lao People's Democratic Republic, Myanmar, Thailand, Viet Nam, adjacent sea and ocean areas

RTH Region	RTH Reference No.	RTH City (Country) (*=RTH/MTN)	RTH's Principal GISC	RTH's Backup GISC	RTH's Area of Responsibility
2	27	New Dehli* (india)	New Delhi	TBD	Bangladesh, Bhutan, India, Maldives, Myanmar, Nepal, Pakistan, Sri Lanka, adjacent sea and ocean areas
2	28	Beijing* (China)	Beijing	Tokyo	China, Democratic People's Republic of Korea, Viet Nam, adjacent sea and ocean areas
2	29	Jeddah* (Saudi Arabia)	Jeddah	TBD	Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, United Arab Emirates, Yemen, other Arabian territories, adjacent sea and ocean areas
3	31	Brasilia* (Brazil)	Brasilia	Washington / Pretoria	Brazil, Colombia, Ecuador, French Guyana, Guyana, Suriname, Venezuela, ships' and aircraft reports
3	32	Buenos Aires* (Argentina)	Brasilia	Washington / Pretoria	Argentina, Bolivia, Chile, Paraguay, Peru, Uruguay, ships' and aircraft reports
3	33	Maracay (Venezuela)	Brasilia	Washington / Pretoria	Colombia, Ecuador, French Guyana, Guyana, Suriname, Venezuela, ships' and aircraft reports
4	41	Washington* (United States of America)	Washington	Brasilia	Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, British Caribbean Territories, Canada, Cayman Islands, Colombia, Costa Rica, Cuba, Curacao, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Monserrat, Nevis, Nicaragua, Panama, Saint Kitts, Saint Lucia, Saint Maarten, Trinidad and Tobago, United States of America

RTH Region	RTH Reference No.	RTH City (Country) (*=RTH/MTN)	RTH's Principal GISC	RTH's Backup GISC	RTH's Area of Responsibility
5	51	Melbourne* (Australia)	Melbourne	Tokyo / Seoul	Australia and outlying islands, Brunei Darussalam, Democratic Republic of Timor-Leste, Federated States of Micronesia, Fiji, French Polynesia, Indonesia, Kiribati, Malaysia, New Caledonia, Papua New Guinea, Philippines, Samoa, Singapore, Solomon Islands, Tonga, Tuvalu, Vanuatu, Wallis and Futuna
5	52	Wellington (New Zealand)	Melbourne	Tokyo / Seoul	New Zealand and outlying islands, Cook Islands, Niue, Pitcairn, Tokelau
6	61	Exeter* (United Kingdom of Great Britain and Northern Ireland)	Exeter	Toulouse	Gibraltar, Greenland, Iceland, Ireland, Netherlands, United Kingdom, ocean weather stations (OWS)
6	62	Norrköping (Sweden)	Offenbach	Moscow / Tokyo	Denmark, Estonia, Finland, Latvia, Lithuania, Norway, Sweden
6	63	Toulouse* (France)	Toulouse	Exeter	Belgium, France, Luxembourg, Monaco, Portugal, Spain
6	64	Offenbach* (Germany)	Offenbach	Moscow / Tokyo	Germany, Jordan, Israel, Switzerland
6	65	Moscow* (Russian Federation)	Moscow	Offenbach / Toulouse	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Russian Federation (in Region VI), Ukraine
6	66	Rome (Italy)	Offenbach	Moscow / Tokyo	Greece, Italy, Lebanon, Malta, Turkey
6	67	Prague* (Czech Republic)	Offenbach	Moscow / Tokyo	Czech Republic, Poland
6	68	Vienna (Austria)	Offenbach	Moscow / Tokyo	Austria, Croatia, Hungary, Slovakia, Slovenia

RTH Region	RTH Reference No.	RTH City (Country) (* =RTH/MTN)	RTH's Principal GISC	RTH's Backup GISC	RTH's Area of Responsibility
6	69	Sofia* (Bulgaria)	Offenbach	Moscow / Tokyo	Albania, Bosnia and Herzegovina, Bulgaria, Cyprus, Former Yugoslav Republic of Macedonia, Montenegro, Romania, Serbia, Syrian Arab Republic

Figure 2 RTH - Areas of Responsibility (* denotes RTH on the MTN)

_____

Annex 6

AMEND THE *MANUAL ON THE GTS* (WMO-No. 386), ATTACHMENT II-15

[These amendments to WMO-No. 386 Manual on the Global Telecommunications System are copied from Annex 3 to Recommendation 3.5/1 (CBS-16)]

A) Proposed amendments to Attachment II-15

The following amendments are proposed for the Att.II-15 of the Manual on the GTS :

1. In "Foreword" (p.144):

"Various protocols were used including X.25 in ~~recent years~~ the 80s and the 90s."

"Considerable efforts have been applied in defining the framework for applying TCP/IP to the GTS ~~and for the orderly transition from the Open Systems Interconnection (OSI) X.25 based origin of the GTS~~. Furthermore, ~~it is understood that~~ TCP/IP ~~will be~~ is now the basis for all new telecommunication functions implemented in support of the WMO Information System (WIS)."

2. In "Introduction / Historical perspectives" (p. 144):

"The GTS at present is predominantly used to support the message switching application using message exchange in WMO format. This exchange is done using~~:~~

~~(a)~~ TCP/IP protocols~~;~~

~~(b) Limited OSI transport service based on point-to-point X.25;~~

and is supplemented by broadcasts."

3. In "Introduction / Purpose of this attachment" (p. 145):

"The aim of this attachment is to describe those aspects of the application of TCP/IP that apply specifically to the GTS to meet new requirements and also the long-established routine data exchange undertaken by MSSs. This attachment ~~takes into account the technical evolution of the GTS from an X.25 based network, and~~ maintains the philosophy that Centres continue to be autonomous as far as possible. It is recognized that the timing for implementation of new systems is determined by individual Members in the light of their available resources and relative priorities, but it is also understood that new WIS functionality is expected to be achieved mostly via TCP/IP protocols."

4. In "Evolution of the GTS" (p. 146):

~~"The use of the ISO/ITU standard X.25 was adopted by WMO in the early 1980s to facilitate the exchange of data and products encoded in WMO binary code forms (GRIB, BUFR, etc.) and to act as a base for higher level OSI applications. Although OSI was regarded at the time as the strategic direction for the evolution of data communications, this has changed. Today, there is no doubt that TCP/IP protocols are the most accepted and widespread protocols for the exchange of data"~~

5. In "GTS DATA EXCHANGE METHODS – Introduction" (p. 156):

"~~There are three data exchange methods defined for used on the GTS. The first two are for the exchange of traditional GTS messages. The third is for the exchange of other data.~~

FTP and SFTP are the two data exchange methods that can be used on the GTS.

~~For traditional GTS messages (those with TTAAii CCCC) the two standards are based on:~~

~~(a) TCP/IP sockets~~

~~(b) FTP.~~

Centres are ~~able to choose between these standards~~ encouraged to choose FTP or SFTP by bilateral agreement. SFTP is to be preferred on the Internet

~~Other data may also be exchanged on the GTS using a separate standard based on FTP~~."

6. In "GTS DATA EXCHANGE METHODS" (p. 156-157):

~~TCP sockets-based data exchange~~

~~The TCP socket standard involves establishing a connection from the sender to the receiver and for GTS messages to be sent preceded by two control fields. The first field contains the message length and the second is a 2-character field indicating message type (binary, alphanumeric or fax). The third field is the actual GTS message contained within a standard GTS SOH/ETX envelope. The receiving centre uses the message length to determine where each incoming message begins and ends.~~

~~The GTS TCP socket protocol does not guarantee end-to-end delivery and data may be lost if the link or one of the message switching systems fails.~~

~~The complete data structure is illustrated in Figure 6. Note that the message length does not include the length of the first two fields (message length and type). The message length must always be eight characters long and include leading zeroes as required. The message type field should be encoded using ASCII characters BI for binary, AN for alphanumeric and FX for facsimile.~~

~~<FIGURE 6>~~

~~The rules for use of TCP/IP socket exchange can be summarized as follows:~~

~~1. All new connections must start from a new message.~~

~~2. Each message is preceded by a message length field of eight ASCII characters and a message type field of two ASCII characters.~~

~~3. Message length is counted from SOH to ETX inclusive and must contain leading zeroes as necessary.~~

~~4. Message type must be encoded as BI for binary, AN for alphanumeric or FX for facsimile.~~

~~5. Receiving centres will check synchronization as follows:~~
~~• Check that the first 8 characters are ASCII numeric;~~
~~• Check that the 9th and 10th characters are BI, AN or FX;~~
~~• Check that the 11th character is SOH;~~
~~• Check that the last character is ETX.~~

~~6. If synchronization is lost the receiver shall break the connection using the following sequence of TCP user primitives:~~

~~• shutdown (to make sure that all data in the TCP send buffer has been transferred);~~
~~• close.~~

~~7. It is recommended to use separate sockets for ASCII and binary messages, and separate connections for sending and receiving. The sender should always be responsible for establishing the connection.~~

~~8. Once a connection is established, it should be maintained.~~

~~9. If there should be a need to close a socket, the procedure should be as follows:~~
~~• shutdown (to make sure that all data in the TCP send buffer has been transferred);~~
~~• close.~~

~~10. This procedure should also be used when an MSS is being shut down.~~

~~11. If the receiving side receives a new unexpected connection request on a port for which it has an established socket, the old socket should be closed and the new socket accepted.~~

~~12. TCP/IP service/port numbers for these connections will be decided by bilateral agreement. The use of reserved ports (1 to 1023) should be avoided. The use of ports above 10000 is recommended.~~

~~13. To reduce the amount of data lost if an established connection fails, the TCP send and receive buffer sizes can be adjusted. The recommended value for the buffer size is 4KByte, however this value may be agreed on a bilateral basis.~~

~~14. To enable detection of message loss, the use of the channel sequence number (CSN) is mandatory. When using the CSN to check for missing messages, the WMO request/repeat procedures should be used to recover these. It may be useful to automate this mechanism to avoid delays caused by manual interaction. In order to minimize data loss, it is strongly recommended that Centres implement a 5-character-long CSN in the future.~~

~~15. The channel sequence number 000 (or 00000 respectively) should indicate an initialization, and should not cause retransmission requests.~~

7. In “GTS DATA EXCHANGE METHODS” (p. 157):

“SFTP/FTP procedures and file naming convention

Introduction

SSH File Transfer Protocol (SFTP) is a secure file transfer protocol based on SSH. There is no official standard RFC. Despite this, SSH (and therefore SFTP) is now widely available and used over the Internet.

File Transfer Protocol (FTP) is a convenient and reliable method for exchanging files, especially large files. The protocol is defined in RFC 959.

The main issues to be considered are:

1. Procedures for accumulating messages into files so as to minimize SFTP/FTP overheads with short messages (applies only to existing message types);

2. File naming conventions for existing message types (existing AHL);

3. General file naming conventions;

4. File renaming;

5 Use of directories;

6. Account names and passwords;

7. SFTP/FTP sessions;

8. Local SFTP/FTP requirements;

9. File compression.

Accumulating messages into files

~~One of the problems with using FTP to send traditional GTS messages is the overhead if each message is sent in a separate file. To overcome this problem, multiple~~ Multiple messages in the standard GTS message envelope ~~should~~ could be placed in the same file according to the rules set out below. This method of accumulating multiple messages applies only to messages for which AHLs have been assigned. “

8. In “GTS DATA EXCHANGE METHODS” (p. 164-165):

Use of directories

Some receiving centres may wish the files to be placed in specific subdirectories. This should be limited to require only that all files of the same type be delivered to the same directory. It is recommended that a separate directory be used for each host system that is initiating SFTP/FTP sessions to avoid the possibility of filename duplication.

Account names and passwords

Using SFTP/FTP, the sender “logs in” to a remote machine using a specific account name and password. The receiving centre defines the account name and the password. There are potential security implications for centres so care needs to be taken.

The following general rules, however, should apply:

(a) The receiving centre defines the user account and password for the sending centre; (b) Anonymous FTP may be used or a specific account may be created. (If anonymous FTP is used, each sending Centre must have its own subdirectory on the FTP server.)

SFTP sessions can also be authenticated using asymmetric keys. NMHS can choose between user/password or asymmetric keys.

SFTP/FTP sessions

To limit the load on both the sending and receiving systems, no more than one SFTP/FTP session per file type should exist at the same time. If, for example, Centre A wishes to send two files to Centre B of the same type (for example, .ua), the second file must not be sent until the first is finished. Centres should limit the number of concurrent sessions with a particular Centre to five maximum.

The idle timer for closing the SFTP/FTP session should be set to a value between the cut-off time for accumulating messages (maximum 60 seconds) and a maximum of 3 minutes.

To minimize overheads the sending centre should keep the SFTP/FTP session connected for at least 10 minutes or until the idle timeout has been reached (subject to bilateral agreement).

Local SFTP/FTP requirements

All sending centres will need to allow for additional “static” FTP commands to be included in the FTP commands that they issue. For example, some Multiple Virtual Storage centres may require the inclusion of “SITE” commands to define record and block lengths. Centres should support FTP commands as specified in RFC 959 unless some are excluded by bilateral agreement. There may also need to be bilaterally agreed procedures and commands.

It is the responsibility of receiving Centres to delete files after they have been processed.

In order to meet the 2-minute maximum delivery requirement for warning messages, centres receiving files via SFTP/FTP should aim to pick up and process incoming files no later than 15 seconds after they are received.

B) Update of Compression Values table 6, Attachment II-15. Manual on GTS

ET-CTS noted that IPET-DRMM had agreed with the proposed changes and agreed to include the following update in the Manual on GTS Attachment II-15 as follows:

ATTACHMENT II-15 should be amend to accepted new compression values in “Table 6. Accepted compression values” of ATTACHMENT II-15 (p. 162), and “Z” compression shall be tagged to ‘deprecated’.

Compression	*Meaning*
Z	DEPRECATED The file has been compressed using the Unix COMPRESS technique
zip	The file has been compressed using the PKWare zip technique
gz	The file has been compressed using the Unix gzip technique
bz2	The file has been compressed using the Unix bzip2 technique
xz	The file has been compressed using the xz technique

C) Update of Table 3. Accepted pflag values

ATTACHMENT II-15 should be updated to include the ability of packing files before transfer (p. 160) include the example and notes as shown below.

Table 3. Accepted pflag values

pflag	*Meaning*
T	The productidentifier field will be decoded as a standard $T_1T_2A_1A_2$ii data designator (The WMO standard data designators are given in Attachment II-5)

A	The productidentifier field will be decoded as a standard Abbreviated Heading, including BBB as appropriate, space characters being discarded,e.g. $T_1T_2A_1A_2$iiCCCCYYGGgg[BBB]
W	WMO Product Identifier
Z	Originating centre's local product identifier
X	Multiple valid GTS files archive, shall be extracted according to the type of the archive.
TM	The productidentifier field will be decoded as a standard T1T2A1A2ii data designator (the WMOstandard data designators are given in Attachment II-5). The file will contain the metadatacorresponding to the related "T" file.
AM	The productidentifier field will be decoded as a standard Abbreviated Heading, including BBB as appropriate, space characters being discarded, e.g. T1T2A1A2iiCCCCYYGGgg[BBB]. The file will contain the metadata corresponding to the related "A" file.
WM	WMO Product Identifier. The file will contain the metadata corresponding to the related "W" file.
ZM	Originating centre's local product identifier. The file will contain the metadata corresponding to the related "Z" file.

Example of file:

X_fr-meteofrance-Toulouse_C_LFPW_20060913030000.tar.xz

This could contain after extraction the following files:

- T_PGBE07_C_KWBC_20020610180000_D241_SIG_WEATHER_250-600_VT_06Z.tif
- W_fr-meteofrance-Toulouse,SYNOP,MAIN+HOURS,,RRA_C_LFPW_20060913030000.txt
- LFPW00000123.b
- LFPW00000124.f
- LFPW00000125.b

[And adding notes:]

a) Use of files archives for FTP exchange is through bilateral agreement of Centres. Any new GISCs should have this functionality from the start of 2018 and any existing GISC's before the end of 2020.

b) For pflag X only compressed archive file format extension is allowed (tar, tar.gz, tar.xz and .zip)

———————

Annex 7 to draft Resolution 5X/1 (EC-69)

AMEND *GUIDE TO INFORMATION TECHNOLOGY SECURITY* (WMO-No. 1115)

[These amendments to WMO-No. 1115 Guide to Information Technology Security *are copied from Annex 4 to Recommendation 3.5/1 (CBS-16)]*

Make the following amendments be made to the *Guide to Information Technology Security* (WMO-No. 1115)

(See http://wis.wmo.int/file=2479 for authors' full text track changes)

1. Under Revision History include:

2016-April – ET-CTS, document review

2. Under 1. Executive Summary

(Paragraph 1)

The quality of ~~our~~ work, ~~our~~ research and ~~our~~ services ~~for~~ supporting ~~the~~ health and safety of humans depends on the exchange of meteorological and environmental data, and on discussions that occur within the WMO ~~our~~ scientific community.

(Paragraph 3)

However, in parallel to these positive changes in the way our community works, an increasing number of threats are prevalent throughout the ~~whole~~ Internet, and …

(Paragraph 5)

For example, it would potentially only take minutes for a newly purchased computer system to become infected with some form of electronic virus if it was ~~installed on~~ connected to the Internet without …

(Paragraph 8)

… It should ~~help to~~ act as an aid to understanding the basic concepts and principles of ITS, …

(Paragraph 9)

– … approach to all ITS matters

– Building a zoned network architecture that will provide resilience against attempts to ~~illegally penetrate~~ compromise systems, networks and hosts. In this context, a zone is a logical area within a networking environment with a defined level of network security

– Monitoring external connections in order to detect any abnormal access or activity

– Regularly applying security patches to critical systems as they become available

– Ensuring that access control mechanisms are in place, commensurate with the system being protected, and ~~M~~managing them with diligence. ~~care the user access codes and passwords~~

– _ _ _ _ _ _ _ _ reinforcing best security and cultural practices across Organisations through continual security education

The complete list as defined in the International Standards Organization (ISO) / International Electrotechnical Commission (IEC) information security standard can be found at http://en.wikipedia.org/wiki/ISO/IEC_27002. ~~Another helpful reference is http://www.itgovernance.co.uk/bs7799.aspx.~~

3. Under 2. Definition of Information Technology Security

The purpose of Information Technology Security (ITS) is to help an organization fulfil its mission by protecting its IT resources, which also include observation systems, and through that, its assets. ~~These assets must be properly identified so that adequate security requirements can be defined.~~

Adequate security requirements can be defined using the following steps:

1. _ _ _ _ Identifying the assets

2. _ _ _ _ Identifying the proper security criteria with, for each criterion, a proper scale (cf. §2.3)

3. _ _ _ _ Identifying the assets' security needs, according to the defined criteria

4. _ _ _ _ conducting a risk analysis (some risks described in § 2.2)

5. _ _ _ _ Identifying the security techniques and procedures to consider (cf. §2.4)

Additional information regarding the information security standard can be found at http://en.wikipedia.org/wiki/ISO/IEC_27002, and http://en.wikipedia.org/wiki/ISO/IEC_27001 and in section five of this document.

The next four sections briefly mention some of the tasks necessary ~~tasks~~ to implement ITS…

4. Under 2.1 Protecting systems against potential failures

All Information Technology (IT) resources play a part, which must be correctly understood, in permitting an organization to deliver services according to its mission. Any failure in these IT resources can then affect the capability to deliver these services.

Moreover, ~~most~~ some organizations have dedicated links with partners. By default, these partner links should be considered similarly to ~~as unsecure as~~ any other public link (such as a ~~the~~ connection to the Internet). They could be used to propagate security threats ~~incidents between organizations. In the best case scenario, these could damage reputation, and, in the worst case scenario, generate legal proceedings~~.

Thus, ITS is concerned …

5. Under 2.2 Malicious versus non-malicious

… For example, malicious activities can include fraud and theft, internal or external hackers, malicious codes such as viruses or spyware, espionage, etc. …

6. Under 2.4 Security techniques and procedures to consider

Once an organization has properly identified its ITS requirements, ~~prevention measures are set up to prevent or restrict an error, omission or unauthorized intrusion~~ measures are implemented to technically and procedurally deliver against them.

Monitoring and reporting should give the organization some ~~proper~~ visibility of its information system. ~~They~~ It must be defined so that a security incident can be ~~quickly~~ detected, ~~and~~ its origin ~~properly~~ identified, and for this to act as an enabler to a complementary process that would limit the threat boundary (such that it is prevented from doing further damage to connected systems/data).

Predefined ~~i~~incident handling and disaster recovery procedures are helpful in minimizing ~~essential to minimize~~ the impact of an ITS-linked ~~incident~~ event within an organization, by reacting quickly and in a proper manner to the incident, and by being able to recover the essential elements impacted ~~by the incident~~.

Once the incident is over, it ~~must~~ should be analysed so ~~that prevention measures can be reviewed~~ potential lessons can be learned ~~if necessary~~.

7. Under 3.1 Reasons for threats

~~The motivations~~ Motives can be deliberate or accidental.

8. Under 3.1.3 Playful or exploration to 3.2.3 Malicious hacking

Another kind of motivation is curiosity, boredom, game or challenge. Many famous governmental institutions have been impacted ~~hit~~ by such ~~motivated~~ attacks, degrading their reputation.

3.1.4 Accident

The last category is human or physical accident or oversight. It can take many forms and touch any part of the information system (network, hardware, ~~and~~ software, procedural), and can be ~~prevented~~ mitigated by adequate ~~disaster recovery~~ procedures and training, such as implementing system redundancy and automatic failover procedures, being aware of public visibility, or delivering regular training.

9. Under 3.2 Common threats

3.2 Common threats

A very resourceful link for this topic is https://www.sans.org/critical-security-controls ~~http://www.sans.org/top-cyber-security-risks/~~.

3.2.1 Malicious codes: viruses, ransomware, worms and Trojans ~~horses~~

A virus is a destructive computer program that spreads from computer to computer using a range of methods, including infecting portable storage (e.g. USB), infected web pages ~~floppy disks~~ and other programs. Viruses ~~typically~~ often attach themselves to a program and modify it so that the virus code runs when the program is first started. The infected program typically appears to run~~s~~ normally, but the virus code then infects other programs whenever it can.

A worm is a special type of virus that does not attach itself to programs, but rather spreads via other methods such as e-mail.

A Trojan~~horse~~ (or backdoor) is a program that performs the desired task, but also includes unexpected functions, such as allowing remote connection to the infected computer or sending information.

All these codes have the potential to disrupt services, destroy information, use resources for their own good, or any other function that the originator of the code may wish to implement.

3.2.2 Denial of service

A denial-of-service attack is characterized by an attempt to prevent legitimate users of a service from using that service. These attacks can be deliberate or accidental, such as abusive use of storage, network and supercomputing resources. They can also be from distributed (and therefore difficult to block) sources, using networks of compromised hosts called a "botnet".

10. Under 3.3.1 Hacking systems …

All these components, if not kept up to date regarding security holes, or if not properly configured, can easily be used by a threat agent (human, such as malicious hackers, or non-human, such as viruses) to compromise the system. If the security hole is not known to the vendor it is known as a zero-day vulnerability. Patches should be applied when they become available.

Specific tools exist, used by security staff as well as malicious hackers, to identify both security holes and configuration weaknesses of a system.

11. Under 3.3.4 Spying …

One of the most dangerous forms of spying is a class of software called keyloggers. Once installed on a computer, these systems can collect every keystroke, mouse movement and screen update on a computer, thus allowing a hacker to obtain all privileged information before it is encrypted or after it is decoded. Keyloggers can also be of the hardware variety, often placed in-line on USB ports, and can use their own wireless connectivity to report what they gather back to an off-site system.

3.3.5 Root or Domain Controller access

Hackers try to get access to the most privileged user or account in order to gain control of the entire network. Avoid keeping the passwords hard coded in the software or saved in flat files or in spreadsheets.

3.3.6 Wireless LAN Networks

Wifi has become an accepted method of connection of mobile devices. Mobile devices connect to a wifi access point to access IP services. These services can be replicated by "imposter" systems to look like official wifi services, but can act very differently. For example, when they are used to access the Internet they can locally show a Web page to be secure when accessed, but the secure access is only to the "imposter" device, not the end website. Users information including their passwords and keys can then be captured in the open, and used to steal personal information and access services.

Users are less likely to be vulnerable if they are accessing internet services through a VPN tunnel to their home organization. The use of split tunnelling (where Internet services are accessed locally) increases the risk and is not recommended for Corporate use.

It is possible for official organizations wifi to detect and suppress these "imposter" access points, but this is unlikely where you do not control the environment. In a public space be vigilant for wifi services which have multiple similar names, or if in doubt, ask someone in charge which service to use.

12. Under 4 Impacts of Threats and Security Events

Although it can be difficult to predict exactly what the impacts can be, the following are key potential impacts, which can be used to prepare security plans and contingency plans. Understanding the potential impacts is also important in justifying the funding for security measures, as the cost of repair, loss of business, loss of reputation and even loss of life often far exceed the cost of ~~defence~~ mitigation measures.

It should also be noted that although some events may seem to be low impact at first, they could be of major importance to an organization at a later date, since many events are just part of a set-up process for later events. In addition, because all organizations will be interconnected, these types of events can be set-ups for attacks in other organizations. In this respect, it is important to note our responsibility to the community of interconnected ~~machines~~ systems.

… 4.1 System and service impacts …

(c) *System or component of system or data destroyed:* The events cause not only the systems and services not to be available for a period of time, but cause the destruction of resources. Typically, this can be the destruction of data on ~~hard disk drives~~ storage media, or stored in the database. Some viruses have been demonstrated to harm hardware by putting it in states that it was not designed to be in ~~used for~~. These problems waste much time, but also require system components to be either replaced or reinitialized. There is often an important cost associated with these repairs.

(e) *System used to compromise others:* The events would compromise an organization's systems in a way that is not detected, and may be left unused for a long time. However, these components can be used to compromise other systems. Although the impact on a given organization may seem negligible, harm to other organizations is possible. Furthermore, hackers often use such techniques to hide themselves behind several layers of obscurity as a ~~of apparently unnecessary hops~~ disguise. These layers render troubleshooting very difficult and provide much hiding space for illicit components. An organization could be falsely accused of being the source of trouble because of this technique.

4.2 Administrative, legal and reputation impacts

In addition to the obvious system and service impacts, all security events can also cause administrative, legal and reputation impacts. By being connected to the Internet, all organizations need to act as good corporate citizens. They must mitigate the problems of security and ensure they are not the cause of problems to others. Failure to do so may eventually lead to legal action. It is also obvious that bad information and poor service will certainly have administrative impacts, as well as the loss of reputation ~~impacts~~. This is particularly important in the weather business, where state agencies have an important responsibility for the health and safety of their citizens.

The perception that a member in the GTS community may be compromised can lead to a series of restrictions or concerns that this may be a threat to connected agencies. Members may isolate one another until further information on the issue is sought. This can take some time as this may involve the national intelligence counterparts. During this period the exchange of critical meteorological information across the world may be disrupted reducing the quality of the services offered.

13. Under 5 Information technology security processes

5 INFORMATION TECHNOLOGY SECURITY PROCESS~~ES~~

The ISO 27000 family of standards helps organizations to keep their information assets secure. ISO/IEC 27001 is the best known standard in the family providing requirements for an information security management system.

These request are described below in more detail.

5.1 …

Security criteria that are important for the organization must then be defined, so that each asset's security needs can be expressed regarding these criteria. The most common ones are availability, integrity and confidentiality.

14. Under 6 Information Technology Security Best Practices

6.1 IT ~~Network and~~ system security

IT system security in this context includes application, operating system, data, and network security. The following paragraphs refer to network and operating system security only. Application and data security will be addressed by an update of this document.

…

Integrity

System integrity is assured through network and system protection, host-based or network-based intrusion detection/prevention systems and an appropriate backup/restore strategy. Data integrity can be assured through cryptographic measures such as hash and signing algorithms.

Confidentiality

Confidentiality is achieved through organization, ~~network, and~~ system~~, protection~~ and cryptographic protection measures.

Accountability

Accountability is achieved through logging of system access and authorization wherever possible.

A key measure for all three security criteria is network and system protection. A key technology for network protection is using firewall systems. The most common use ~~application~~ for firewall systems is a central firewall between the internal network and the Internet based on a proper zoned design. However, depending on the complexity of the internal network, distributed firewall systems should be put in place to protect sensitive internal network zones and systems, for example, databases and servers running critical services, from more dangerous parts, for example, network zones connecting user personal computers (PCs) and workstations (see section 6.2). Network protection can also be improved by introducing an intrusion detection/prevention system (IDS/IPS) to monitor the network traffic at certain points and to detect unwanted or suspicious traffic according to the security policy (section 6.5).

System protection is more complex. The following measures have to be taken:

(a) *Access control:* Make sure that only authorized personnel have both physical and electronic access to a system. In addition, authentication has to be ~~as strong as possible~~ of appropriate strength (appropriate password policy, certificate- or token-based authentication). Finally, logging is important to trace user activity, especially on mission critical systems. Hence, group-based accounts should be avoided wherever possible (where a single account is used and the password shared between users).

(b) *Minimize services:* Disable all services and processes that are not necessary for system operation and service offerings. ~~Run only one single service on critical systems such as Domain Name System (DNS) servers, web servers, etc. Do not combine multiple services whenever possible.~~

...

(e) *Diversification and redundancy:* Make mission critical services, such as DNS servers, customer-related web and File Transfer Protocol (ftp) servers, database servers, e-mail relays, etc., redundant. Make sure that these redundant servers and gateways are physically separated to protect the overall system from fire, flooding, etc.

6.2 ...

Virtual networks can be set up on top of physical networks or other virtual networks. There are numerous types of virtual networks. The most popular are:

– VLANs: Virtual LANs are used to segment a LAN-based Intranet into different network zones; a VLAN is built on top of a LAN and is based upon Ethernet packet tagging according to the Institute of Electrical and Electronics Engineers (IEEE) standard 802.1q.

– VPLS: Virtual Private LAN Service is a way to provide Ethernet-based multipoint to multipoint communication over IP or MPLS networks.

...

~~Be careful~~ Care should be taken with encrypted virtual networks such as IPSec-based VPNs that are set up in tunnel mode versus VPNs in transport mode, which make use of data signing only. Because data are encrypted, virus scanners, intrusion detection/prevention systems and other centralized security measures may ~~do~~ not work. ...

6.2.1 ...

... while a PC is always at risk of Internet worms, Trojan horses and other malicious software.

The host (or PC) in the internal network must strictly follow the security policy of the corresponding network zone, and invalid external connection detection software should be installed in the host which could access the critical IT resource. The LAN segments that connected most critical IT resource or the sensitive data should be physically isolated by the local law.

To protect the disjunctive network segments from each other, they should be interconnected through appropriate ~~firewall~~ separation systems.

The security of an Ethernet LAN or LAN segment can be increased by using ISO/OSI (Open Systems Interconnection) layer 2 switching technology instead of broadcast media, so that traffic from a host A to another host B cannot be sniffed by a third-party host C. However, layer 2 switching cannot avert the so-called Address Resolution Protocol (ARP) spoofing. Additional security measures, such as Port Based Network Access Control in conjunction with

the use of host certificates, either based on registered hardware addresses or as defined in IEEE standard 802.1x have to be taken into consideration to protect LANs from such attacks. Port-based access control makes sure that hosts which have not been registered cannot be connected to the network.

~~6.2.2 Wide Area Networks~~

~~A WAN interconnects a number of local networks that can be LANs or other WANs, for example, Metropolitan Area Networks. In this context, a VPN can also be seen as a WAN.~~

~~Typically, WANs are public or semi-private networks that are used by different companies, public offices or even private people. Furthermore, a WAN has to carry multiple protocols mostly making it impossible to apply certain filters that comply with the demands of all users.~~

~~Therefore, WAN security can mostly be considered low. Measures have to be taken to protect a private Intranet against public WANs. These measures are referred to as firewalls or firewall systems.~~

6.2.~~3~~2 Wireless Local Area Networks

Securing Wireless LANs (WLANs) ~~are very critical with~~ is critical in regards to availability, integrity and confidentiality:

– *Availability:* …

– *Integrity and confidentiality:* Cryptographic measures have to be taken to guarantee data integrity and data confidentiality, if required. In particular, authentication data such as user names, passwords and token codes have to be encrypted to avert scanning and spoofing. One such method could be using IEEE 802.1x.

The following measures have to be taken to protect WLANs and other network zones that are connected to WLANs:

– *WLAN footprint:* Make the reception area of a WLAN (footprint) ~~as small as possible~~ match only the area of intended coverage. Make sure that WLAN radio cannot be received outside desired borders. Use a WLAN radio scanner to verify.

– *Radio shielding:* …

– *Encryption:* Use encryption on WLANs. Choose the best available encryption algorithm and change the default settings before activating WLANs. ~~Do not rely on standard encryption (Wireless Application Protocol (WAP), IEEE 802.11i) for mission critical WLANs.~~ For user authentication and data encryption, …

– …

– *Intrusion detection:* If necessary, install an IDS/IPS for additional security. Note that an IDS/IPS does not work well for encrypted network zones. However, the IDS/IPS can monitor communication relations and can generate alarms in case of illegal activity up to ISO/OSI layer 4, for example, port scans.

– *Protecting access:* Mechanism to protect the Wireless Network to unauthorized access must be used. This includes, for example, 802.1x or WPA2.

6.2.~~4~~3 Firewall systems

Firewalls can be divided into two major groups:

– Packet filters

– Application Layer and rule based (also known Next Generation firewalls) Gateways

Packet filters control network traffic …

…

While a firewall always reassembles incoming IP packets to prevent attacks caused by fragmentation, access lists on routers do not reassemble fragmented packets. Therefore, access lists cannot always be considered as a substitute for a firewall.~~.~~

6.3 Remote access

Remote access to network resources is one of the most critical applications with regards to network security. Remote-access systems can be:

– Plain Old Telephone Systems, Public Switched Telephone Networks or Integrated Service Data Networks dial-in servers

– Secured Internet access (IPSec- or SSL-based VPN gateways)

~~– Wireless access servers (for example, Bluetooth)~~

There are four items that have to be taken into consideration when designing and operating remote access:

(a) *Network architecture:* …

(b) *User authentication:* In particular, for remote-access systems, proper user authentication is essential for overall network security. Strong authentication mechanisms such as certificate- or token-based or multi-factor methods are preferred over weak, password-based methods.

(c) *User authorization:* Make sure that even authenticated users will not obtain access to all systems. Authorization rules have to be in place to limit access to systems that the user is authorized for. For easy maintenance, authorization should be based on groups rather than on per-user rights. A user may be a member of several groups, granting the individual all the rights of each group. The host, that is being by an authorized user to get access to an internal system, should meet the security requirement.

(d) *Logging and accounting:* …

6.4 Server access and security

…

– The servers are well patched against all known security holes. Make sure that the latest patches have been applied. ~~Verify the p~~ Patches should be ~~before~~ verified in accordance with change and configuration management processes prior to being installed~~ing them~~ (especially on mission critical systems).~~.~~

In addition to authorization mechanisms, …

… Systems that serve anonymous users should be separated from pre-authorized systems that store confidential data. They should be located in separate firewall zones. Never operate both anonymous and pre-authorized services on one single machine.~~:~~

…

6.4.1 File system authorization rules

Both anonymous and pre-authorized systems require strict authorization rules. By default, only read access should be allowed. Write access should only be allowed when required. Systems with write access should have dedicated directories to store the data and to scan for viruses and malicious code before making them available to internal resources or users.

~~Finally, make sure that directory and file visibility rules are in place. Hide as much information as possible and only make information visible to the remote user required to successfully use the service offered. This also comprises directory and file access rules. Make sure that private files and directories cannot be accessed through fraudulent user behaviour such as directory traversal attacks.~~

Sometimes, it might be required to only accept signed data to verify data integrity. Unsigned data …

6.5.2 Developing a policy

…

Finally, policies should be approved and signed by an appropriate ~~a high~~ authority in the organization. Again, since security is the matter of several (if not all) components of an organization, only ~~a high~~ such an authority will ensure consistency in approach and in implementation.

…

6.8.2 New system installation and change management

All new systems or new system components should be introduced in the production environment through a predefined installation procedure. This procedure should include at least the following steps:

– Suppress all the accounts that do not have passwords

– Back up all configuration files

– Ensure software is up to date according to the organizations configuration and version control processes, and keep a list of components and version numbers

– Suppress network services that are not necessary

– Configure and install a logging system for all important system activities

~~– Use shadow passwords and limit validity of passwords~~

All changes should be tracked to control the system components and be capable of tracing unwanted changes.

6.8.3 Installation of security patches

Follow the security advisories from the Computer Emergency Response Team (CERT) (for example, http://www.us-cert.gov, http://www.dfn-cert.de, https://www.cert.be or http://www.cert.ssi.gouv.fr) and install patches as soon as they are available.

6.8.4 User account management

– All accounts must belong to a specific user.

– Each user should read and understand the organization's security policy.

– End-users' ~~User~~ accounts that are unused for a period of time (3 months) should be deactivated.

~~– Password crackers should be run on a regular basis to identify easily cracked passwords and notify the users to change these passwords to more difficult ones. However, be aware to pay attention to possible legal issues! Best practise is to inform the users about regular password checks and let them individually sign a declaration of agreement, for example, in terms of a common IT user policy before running any password cracking tools.~~

– A password policy should be defined, which outlines the requirements for password complexity, strength, and duration; this policy should be known by all users. ~~Passwords must be changed on a regular basis (at least every 3 months).~~

– Remote-access users should use one-time password systems to eliminate the possibility of password capture by illicit users.

~~– Users should be informed of what constitutes a good password.~~

6.8.5 Backup/restore procedures and regular testing …

6.8.6 Detection procedures

Several detection procedures can be put in place to monitor system activity and possible illicit or unwanted activity. These procedures should be 24/7 and can include intrusion detection and prevention, abnormal system activity detection, vulnerability scanning, loss of system or loss of data procedures.

6.8.6.1 Protection from ~~viruses~~ malicious code

Real-time anti-virus systems should be installed and applied ~~on all operational computer equipment~~ where appropriate. Whole-of-server scans should be run on a daily basis. Anti-virus software should be configured in real-time mode to ensure any infections are identified and cleaned immediately upon detection.

A separate server or computer should be configured to sit inside the organization's firewall in real-time mode. This server should be configured with appropriate software to check for ~~viruses~~ malicious code. If ~~a virus~~ such code is detected and all incoming and outgoing e-mail attachments can be cleaned, then the message can be distributed. If attachments cannot be cleaned, then the message should be blocked.

~~Anti-virus software should be regularly updated with new definition files. Anti-virus software should be regularly reviewed. It may be necessary to use more than one type of scanning software to ensure that maximum protection is provided for all information platforms and environments. Organizations should ensure that virus protection and recovery strategies are included in risk management and business continuity plans.~~

Typical controls to protect against malicious use technology, policies and procedures, and training, applied in a layered manner from perimeters inwards to hosts and data. They should be applied at the host, network, and user level.

6.8.6.2 User education

...

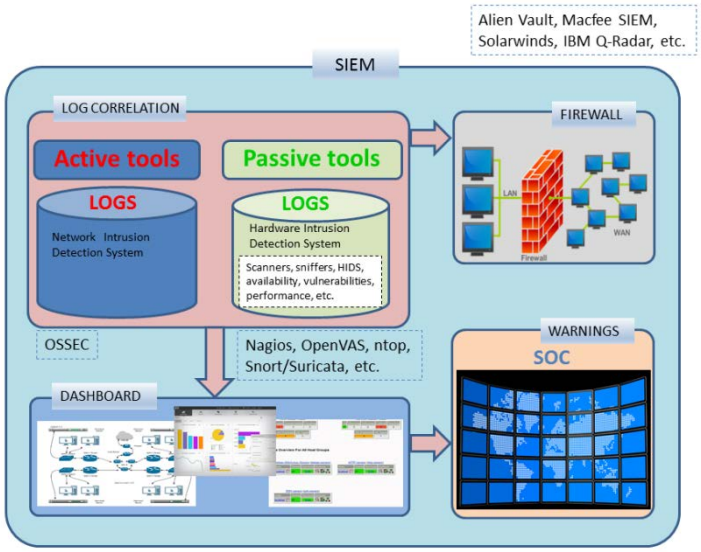
6.8.8 Security information and event management

It is recommended to implement a solution capable to monitor, evaluate and correlate events related to security issues. This type of solution, known as SIEM - Security Information and Event Management, is a software-based solution, which combines events and alerts, provides by network agents in real-time mode. It behaves as a “land mine” in front of your system and helps you visualize or pay attention on what is going on and take actions in advance.

A SIEM solution allows events generated by various security applications (such as firewalls, proxies, intrusion prevention systems and antivirus) to be collected, normalized, stored and correlated in order to enable a rapid identification and response to incidents. A standard SIEM tool would include the following topics:

- Combine the features offered in both technologies SIM (Security Information Management) and SEM (Security Event Management). Real-time access, centralized and consistent to all logs and security events, regardless of the technology and manufacturer;
- Correlation of heterogeneous technologies logs, connecting common or significant attributes between sources, in order to transform the data into useful information;
- Identification of behaviours, incidents, fraud, anomalies and baseline breaks;
- Alerts and notifications triggered automatically in the event of non-compliance with security policies, regulatory standards or according to pre-established business rules;
- Sophisticated reporting on environmental safety conditions for SOC (Security Operations Centre) teams auditing and incident response;
- Retention and indexing long-term data allowing subsequent forensic analysis;
- Auditing event log related information.

The concept of a SIEM system can represented as indicated in the picture:



6.9 Public server configuration

...

It is very important to minimize risks by securing such servers. Here are a few good practices:

(a) Architecture: Install the server in a ~~DMZ~~ dedicated zone, for example, a semi-private network that is visible through the network's firewalls, but that is not part of the private networks of an organization;

(b) Filtering:

(i) Protect the server from network access by a firewall filtering all network ~~fluxes~~ flows, but the port used by the service to access the server;

(ii) ...

(c) Bandwidth: A bandwidth management tool should be used to avoid excessive use of bandwidth by a single user (or group of users);

(d) System/application:

(i) The server should process as few types of data as possible (for example, do not combine multiple server applications on the same virtual or physical system);

(ii) The server should be stripped of all unnecessary services and applications, see also section 6.1 for system security;

(iii) ...

_____

Annex 8

AMEND GUIDE TO VIRTUAL PRIVATE NETWORKS (VPN) VIA THE INTERNET BETWEEN GTS CENTRES (WMO-No. 1116) (AVAILABLE IN ENGLISH ONLY)

[These amendments to WMO-No. 1116 Guide to Virtual Private Networks (VPN) via the Internet between GTS centres *are copied from Annex 5 to Recommendation 3.5/1 (CBS-16)]*

Make the following amendments to the *Guide to Information Technology Security* (WMO-No. 1115) and the *Guide to Virtual Private Networks (VPN) via the Internet between GTS centres* (WMO-No. 1116)

(See http://wis.wmo.int/file=2481 for authors' full text track changes)

1. Under 2.2 Types of virtual private networks

(i) Asynchronous Transfer Mode (ATM) and Frame Relay connection;

(ii) Multiprotocol Label Switching;

(iii) Virtual Private LAN Service;

(iv) Link-Layer Encryption (Layer 2 Tunnelling Protocol (L2TP) or Point-to-Point Tunnelling Protocol (PPTP));

2. Under 2.2.1.1 Asynchronous Transfer Mode and Frame Relay

Following the definition of VPN given in chapter 1, early data network, such as ATM and Frame Relay solutions, must be considered as VPNs. ~~By construction, a Frame Relay (and ATM) network, such as the Regional Meteorological Data Communications Network (RMDCN), is a VPN. The provider Orange Business Services (OBS) has a network that is securely divided among all customers. Therefore, on a global telecommunication system, multiple isolated sub-networks coexist.~~ In this case, the VPNs rely on the operator.

3. Under 2.2.1.2 Multiprotocol Label Switching

This solution is now widely offered by operators.

Virtual Private LAN Service

VPLS is a way to provide Ethernet-based multipoint-to-multipoint communication over IP or MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudo-wires, and VPLS allows any-to-any (multipoint) connectivity.

4. Netscape created the protocol SSL. In the TCP/IP layering model it is on top of the TCP layer. Therefore, it could be used for adding security (strong authentication and encryption) for all TCP-based application (telnet, File Transfer Protocol (FTP), etc.). SSL is no longer recommended for use, all SSL versions are deprecated by now. The recommended protocol is now TLS. Companies use this technology to provide secure remote access to their internal infrastructure by using SSL/TLS VPNs with additional strong authentication, Under 2.2.2.1 Secure Socket Layer and Transport Layer Security

4. Under 3.1 Internet Protocol Security architecture

From RFC 2401 (~~now~~ replaced by RFC 4301; Kent and Seo, 2005; RFC 4301 partly replaced by RFC 6040, Briscoe, 2010 and RFC 7619, Smyslov and Wouters, 2015):

5. Under 4.2.1 Physical layers

– Frame Relay lines: The leased line is replaced by a connection to a Frame Relay network, but only two peers share the same Frame Relay network

– An MPLS network such as the RMDCN (as WIS core network) ~~in Region VI~~ is such a network

– Connections using the Internet

– Satellite communication channels

...

With the growth of products and data, and with the ~~upcoming Weather~~ WMO Information System (WIS) network, National Centres (NCs), Data Collection or Production Centres (DCPCs) and Global Information System Centres (GISCs) will want to exchange much more information. ...

_____

BACKGROUND INFORMATION SUPPORTING DECISIONS/RESOLUTIONS/RECOMMENDATIONS

NOT TO BE INCLUDED IN THE SESSION REPORT

References:

1. *[Link to the full report on the website]*

2. .....

Introduction

[Comment: Main points and arguments leading to formulation of draft decision presented in this document]

First sub-title

Second sub-title

1. .....

(a) .....;

(i) .....;

- .....

2. ...